Blockchain Standard: Can We Reach Consensus?

Vincent Gramoli
University of Sydney
Data61-CSIRO
vincent.gramoli@sydney.edu.au

Mark Staples
Data61-CSIRO
School of CSE, UNSW
mark.staples@data61.csiro.au

Abstract

In this paper, we study ongoing blockchain and distributed ledger technologies (DLT) standardization. To this end, we list standard organizations and the efforts they devote to standardise blockchain and DLT. We then identify a lack of terminology that can hamper communication on this topic and propose clarifications to address these ambiguities. Finally, we propose a high level description of blockchain and DLT by describing three elements of their functional architecture.

1 Introduction

Blockchain technology (or more broadly, distributed ledger technology) can securely record, audit and transfer the ownership of digital assets. It initially emerged as infrastructure in a solution to the problem of digital cash. Blockchains allow the automation of cross-border payments over the Internet regardless of geographical constraints [12]. This contrasts with conventional financial transfers that can take days between different banks, especially when they operate in different countries. The openness of blockchain technology and its foundations in the Internet make it inherently global. The potential for blockchain extends beyond cryptocurrency, allowing tradeable digital tokens representing physical or digital assets. This expands the theoretical range of application of blockchain technology to many business problems in almost any industry and sectors, including fincancial applications, supply chain, Internet of Things (IoT), etc.

However, the pace and extent of the adoption of blockchain technology is hampered by interoperability challenges. These challenges arise not just in relation to choices about the representations of cryptocurrency and digital tokens, but also through fundamental differences in treatments of transaction management. This can make it more difficult for blockchains to interoperate with each other, and also to integrate with conventional enterprise information systems. This may ultimately cause problems for regulatory acceptance of blockchain.

One of the main potential benefits of standardization is improved interoperation, by providing a common and clear shared technical foundation for industry. For blockchain technologies, this may dramatically shift their level of adoption in the global digitally-enabled economy of goods and services.

A major standardization initiative has been initiated on blockchain and distributed ledger technologies through a technical committee of the International Organization for Standardization, ISO/TC 307, and is summarized in Section 4. This goal is ambitious and the focus is broad. Other organizations like IEEE[1] and the ITU[2] have also established standardization efforts on blockchains. Part of their motivation is to identify the needs and responsibilities of their members and stakeholders as users, developers, and operators of this new technology.

Standardization provides a basis for technology investment and economic activity. Thus, these standardization efforts should be based on best practice and be readily applicable. Blockchain technology is a new technology, and best practice is still rapidly evolving. So there are questions about whether it may be premature to standardise blockchain technology. Nonetheless, although blockchain technology is new, it is part of established traditions in computer science. This paper draws on the academic literature and a research perspective to discuss technology options relevant for blockchain standardization. We do not tackle the entire scope of blockchain standardization, but instead focus on foundational issues of a unified terminology, blockchain transaction representation, execution, and security.

Section 2 lists existing standardization efforts. Section 3 identifies some sources of confusion, motivating the need for a standard terminology. Section 4 discusses some issues relevant to blockchain standardization, related to three main function elements: consensus, security, and ownership. Section 5 concludes.

2 Blockchain Standardization Landscape

The perceived need for blockchain and distributed ledger technology (DLT) standards has led to many organizations initiating standardization efforts. A timeline for this is depicted in Figure 1.

International organizations. Major international organizations have created formal activities to work on the standardization of blockchains and DLT.

- **ISO.** The International Organization for Standardization develops and publishes international standards. The ISO has created a Technical Committee, ISO/TC 307, for Standardizing Blockchain and Distributed Ledger Technologies, whose Secretariat is led by Standards Australia. It has a number of working groups and study groups, and is developing standards and other work items related to Terminology, Architecture, Taxonomy

[1] `https://blockchain.ieee.org/`

[2] `https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/q14.aspx`

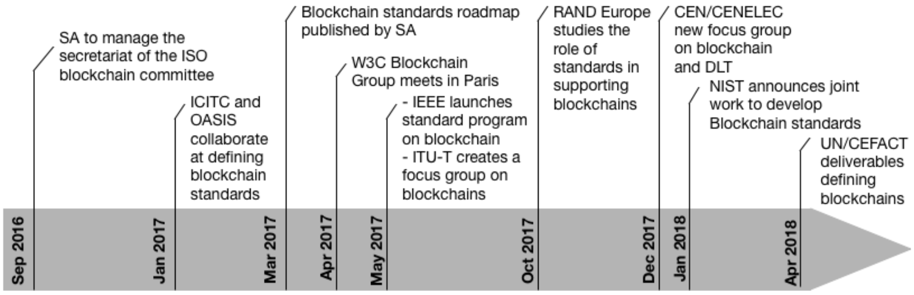
SA to manage the secretariat of the ISO blockchain committee
ICITC and OASIS collaborate at defining blockchain standards
Blockchain standards roadmap published by SA
W3C Blockchain Group meets in Paris
- IEEE launches standard program on blockchain
- ITU-T creates a focus group on blockchains
RAND Europe studies the role of standards in supporting blockchains
CEN/CENELEC new focus group on blockchain and DLT
NIST announces joint work to develop Blockchain standards
UN/CEFACT deliverables defining blockchains
Sep 2016
Jan 2017
Mar 2017
Apr 2017
May 2017
Oct 2017
Dec 2017
Jan 2018
Apr 2018

Figure 1: Various organizations have started devoting efforts to standardise blockchains and DLT

and Ontology, Smart Contracts, Privacy, Security, Identity, Governance, Interoperability, and Use Cases.

- **ITU.** The International Telecommunication Union (ITU) is an agency of the United Nations that produces recommendations and norms defining the interactions of telecommunication networks. One of its three divisions, the Telecommunication Standard Sector (ITU-T), has created a Focus Group (FG) on Application of Distributed Ledger Technology (DLT) *(i)* to identify and analyse DLT-based applications and services, *(ii)* to draw up best practices and guidance which support the implementation of those applications and services on a global scale, *(iii)* and to propose a way forward for related standardization work in ITU-T Study Groups.

- **W3C.** The World Wide Web Consortium (W3C) is a non-profit international standardization organization whose member organizations collaboratively develop Web standards. They have initiated a blockchain community group to *(i)* generate message format standards for blockchain based on ISO20022[3]; *(ii)* generate guidelines for usage of storage including torrent, public and private blockchains, side chain and CDN; and *(iii)* study and evaluate new technologies and use-cases such as inter-bank communications.

- **IEEE**. The Institute of Electrical and Electronics Engineering (IEEE) is a non-profit professional organization that develops standards and has created an ongoing project related to blockchains, called the Standard for the Framework of Blockchain Use in IoT[4] and an industry connection document, the Blockchain Asset Exchange[5] as well as an active working group[6] on the topic.

[3] `https://www.iso20022.org`.

[4] `http://standards.ieee.org/develop/project/2418.html`.

[5] `IC17-017-01:BlockchainAssetExchange(PDF,187KB)`.

[6] `https://standards.ieee.org/develop/wg/blockchain.html`.

- **IETF** The Internet Engineering Task Force (IETF) is an informal open group that designs Internet standards. It plays a major role in defining the Internet protocol suite that is used for network communications and interoperability standards by publishing Request For Comments (RFC) documents that can impact blockchain technologies.[7]

Regional organizations. Below we list the recent efforts of regional organizations in trying to standardize blockchain and DLT.

- **Standards Australia (SA).** Standards Australia is a non-government non-profit Standards organization who is responsible in the development and adoption of standards in Australia by forming technical committees bringing together relevant parties and stakeholders to reach consensus. Standards Australia leads the Secretariat for ISO TC/307.
- **ISTIC Europe**. The International Securities Association for Institutional Trade Communication (ISITC) Europe, is a non-profit organization promoting operational efficiency, harmonization and education in the capital markets space. It has created the Blockchain Distributed Ledger Technology (DLT) Working Group to provide a platform for the securities industry players to educate, discuss and validate the emerging Blockchain (or Distributed Ledger) technologies and its role in security processing. With the Organization for the Advancement of Structured Information Standards (Oasis), they are defining technical standards for blockchain/distributed ledger technologies.
- **RAND**. The Research ANd Development (RAND) corporation is a non-profit global policy think tank to offer research and analysis to the US Armed Forces and is financed by the US government and private endowment, corporations, universities and private individuals. RAND, through its European branch, prepared a report[8] for the British Standard Institution, the official standards body for the UK and argues for standardizing the technologies neither early to avoid constraining application nor late to avoid missing opportunities.
- **CEN-CENELEC**. The European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC) aims at fostering the European economy and consider themselves as business catalysts by setting common standards of safety and quality. The CEN CENELEC started a new focus group on blockchain and distributed ledger technologies. The objective of the focus group is, among others, to identify potential specific European standardization needs, notably in support to the current standardization activities being developed in ISO/TC 307.

[7] `https://www.internetsociety.org/issues/blockchain/`.

[8] `https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2223/RAND_RR2223.pdf`.

- **NIST**. The National Institute of Standards and Technology is a measurement standards laboratory and a non-regulatory agency of the US Department of Commerce with a mission to promote innovation and industrial competitiveness. At the beginning of 2018, NIST announced that it will collaborate with ISO in order to define blockchain standards. This announcement happened during a discussion with the Congressional Blockchain Caucus that is interested in how blockchain technology can improve US government services.

- **UNECE**. The United Nations Economic Commission for Europe (UNECE) is a regional European commission of the United Nations. One of the UNECE bodies is the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT), which defines standards relating to trade facilitation and electronic business. It is studying the use of blockchain for trade-related use cases and wrote a white paper[9] on the topic.

This list that starts with the effort of Standards Australia is likely not exhaustive, but indicates the multiple efforts devoted internationally on blockchain and DLT standardization. This multiplicity in the efforts demonstrate a crucial need for communication about blockchains.

3 Agreeing on a Terminology

Communicating about blockchain is key to its standardization. However, the lack of common terminology is a barrier. For example, terminology was recently identified as one of the first priority areas by ISO/TC 307.

Blockchain. A *blockchain* is simply an abstraction that consists of a sequence of blocks. The blockchain is distributed, meaning that multiple *machines*, i.e., computers or computational devices, maintain a local copy of this blockchain. We refer to them as *replicas* as they replicate the blockchain. The distributed nature of these replicas provide tolerance to some replica failing by crashing, however, links between blocks are necessary to guarantee the tamper-proof nature of the replicated information.

There exist many blockchain systems that implement this simple abstraction. Prominent ones include Bitcoin, Ethereum and Ripple. *Users* of a blockchain can record simple *transactions* as transfers of digital assets from an account to another. In some blockchains, users can invoke *smart contracts* as programs that define conditional actions on digital assets controlled by the smart contract. The seminal Bitcoin blockchain [12] allows the chain to fork in a tree, and relies on market incentives to encourage that a growing prefix remains a "chain" with high probability. Since that time, the term "blockchain" has also been used to

[9] `https://www.unece.org/fileadmin/DAM/cefact/cf_plenary/2018_plenary/ECE_TRADE_C_CEFACT_2018_9E.pdf`.

Term	Definition
Block	A data structure that either is a genesis block or contains at least an ordered set of transactions and the cryptographic hash of the content of the previous block.
Blockchain	A sequence of blocks, linked through the cryptographic hash values in those blocks.
Client (resp. *Server*)	A machine that requests (resp. provides) a service from (resp. to) another machine.
Consensus	Agreement among a distributed set of machines on the contents of a block at a given index of the blockchain.
Synchrony	An assumption under which all network messages are delivered within a known time bound.
Pseudonymity	The property of a system where users are identified only through their pseudonym.

Table 1: Some important terms that lack standardised definitions

describe acyclic graph representations of blocks. This may cause some confusion as these representations do not resolve to a sequence or chain.

Clients and servers. Some machines, often called *miners*, have the task of creating new blocks. Initially, the blockchain contains one block called the *genesis block*. Miners gather transactions or contracts through a network (often the Internet) and try to encapsulate them into a new block. They append the block to the blockchain, miners also include in this block the result of a *hashing function* applied to the last block of the blockchain and communicate this new block to the replicas. These miners act as *servers* as they provide the service of treating the requests and storing corresponding transactions into blocks appended to the blockchain. This is in contrast with a *client* who would simply request the service by sending a transaction to a server.

In the peer-to-peer research literature, machines that play the role of both the client and server are called *peers* because they play an equal role by offering and requesting the service at the same time. In the blockchain context, confusion may arise because the term “client” may sometimes denote a server. Examples of this usage are the go-lang Ethereum client also called the `geth` “client” which can function as a miner in Ethereum.

Consensus. In order to guarantee that the blockchain remains a chain, miners must reach a *consensus* on the unique block to be appended after the last block. The seminal approach to agree upon a block at a given index was surprisingly simple: *Nakamoto consensus* consists of each client selecting as the blockchain the longest branch among the existing ones they have observed. This approach guarantees that all nodes reach an agreement regarding the block to be appended provided that they all wait for strictly longer than the time it takes for every block of this index to be propagated to the entire network. Note that this consensus protocol hence requires what is called *synchrony* in that every message gets delivered within a time bound known by all nodes.

The distributed computing literature formalizes traditionally the consensus problem among a distributed system of n consensus participants that all propose a value for a given consensus instance. This is in contrast with the Nakamoto consensus approach, which uses proof-of-work to select the participant that can create and propose a valid block for a given index. This has led to the confusion that proof-of-work is a consensus algorithm, and that similar participant selection mechanisms like proof-of-* are also consensus algorithms. These proof-of-* mechanisms are simply ways to define the n consensus participants that propose blocks (or values in the distributed computing terminology) but are not ways of uniquely determining the correct block for a given index of the chain.

Pseudonymity. The task of mining is typically rewarded with a fee withdrawn from the account of the user issuing the transaction or invoking the smart contract. Public blockchains typically rely on authentication from public-key cryptography. Let us take a transaction request as an example. All users must own a pair of inter-dependent keys: a *public key* shared with others, and *private key* kept secret. When a user requests a transaction to transfer a digital asset from their account to another account, they sign the transaction by encrypting it with the private key, then send it to the miners. The miners check that the transaction was authorized by trying to decrypt (or verify) the signature with the corresponding public key: if this verification succeeds the signature is *valid* and the transaction can be added to a block, else it is *invalid* and the transaction is ignored.

As the identity check consists only of checking that the signature corresponds to the public key, public blockchains typically do not provide a way to confirm the identity of the human user that requests the service. Thus the public key becomes a "pseudonym" for the account of the user. This led to the confusion that blockchains provide anonymity. It is important to understand though, that this mechanism is not sufficient to fully anonymize the requester: machines can infer personal information about a user (like geographical location) by recording the IP address of the requester machine. This is in contradiction with the definition of anonymity as the "characteristic of information that does not permit a personally identifiable information principal to be identified directly or indirectly" [1]. Without additional mechanisms, these blockchain only provide what has been called *pseudonymity*, but do not provide full anonymity.

4 Elements of a Functional Architecture

A complete functional architecture is beyond the scope of this paper. Instead, we focus on three high-level functional elements.

1. **The consensus element:** ensures that a distributed set of machines proposing blocks at a given index of the chain agree on exactly one of these blocks to be appended. One can view this as a distributed voting process that leads to a global decision about the contents of the blockchain.
2. **The security element:** is important to prevent malicious users from tampering with ownership of assets managed by the blockchain. The key security mechanisms are for authentication and integrity.
3. **The ownership element:** tracks ownership through records associating data to addresses or accounts.

For each of these functions, in the following sections we discuss technology options and some issues relevant to standardization.

4.1 Consensus element

Consensus is a fundamental function of a blockchain. If blockchain participants disagree on the block to append to a given index, then it can cause disputes about the current state of the chain. This may lead to *double spending*, a state in which two conflicting transactions happened. As consensus decisions entirely define the current state of ownership of digital assets on a blockchain, they convey some governance power to those who make these decisions.

Blockchain systems select the participants that decide upon the next block by applying conditions typically on the result of the computation issued by some machines, their resources, or simply an attribute of these participants. For example, in the proof-of-work of Bitcoin [12], the deciders are the participants who first solve a difficult cryptographic puzzle. There exist other forms of selection, that rely or different resources, such as coins owned, or randomization [6]. Consortium and private blockchains typically uses a predetermined set of participants that can decide, which may be considered unfair in a large context. Community blockchains [14] aim at bridging the gap between public and consortium blockchains by changing the set of deciding participants at runtime so that all nodes eventually decide upon "some" block but not all waste resources trying to decide upon "all" the blocks.

It is unclear whether these leader selections are ideal. In addition to the direct financial rewards, there are strategic incentives that are also of interest. On Bitcoin, miners have consolidated their computing power into large mining pools and share rewards to reduce the variability of mining rewards. However, this kind of centralization is in contrast with the decentralised ideal of public blockchains. Uniform randomization poses other problems related to the lack of incentivization.[10] Treatments of accountability could help blockchain designers and standardization bodies to find a better balance. Existing standards like ISO 37001:2016 for anti-bribery can be helpful for introducing accountability.

[10] https://www.coindesk.com/no-incentive-algorand-blockchain-sparks-debate-cryptography-event/.

Properties	**Byzantine [10]**	**Reactive [12]**	**Blockchain [5]**
Scalable	✗	✓	✓
Secure	✓	✗	✓

Table 2: Three classes of consensus techniques with different properties

Consensus strategies. As depicted in Table 2, one can identify three types of consensus problems. Some blockchains are proactive but costly in that all but one of the blocks proposed at a given index by the participants are ignored. They solve the *Byzantine Consensus* problem [10].

Most common blockchains, however, use a *Reactive Consensus* because they do not prevent duplicated blocks at the same index, but get rid of duplicated blocks when they are discovered, ensuring eventually that at each index of the chain one block remains [12]. These techniques usually rely on the assumption that global information will be gathered sufficiently fast. This, however, exposes these blockchains to security vulnerabilities in case of unexpected network delays.

More recent blockchains solve the problem of scalability by solving the *Blockchain Consensus* [5] and leveraging the proposals of more participants [7]. High scalability will be key to the success of global blockchain systems and should be a natural requirement of modern blockchains. This type of consensus differs from previous approach but still guarantees the uniqueness of a block at a given index without the cost of solving the Byzantine Agreement. Instead it relies on the identification of all transactions that are valid. This consensus component is tightly related to the security component and the way transactions are validated.

4.2 Security element

A blockchain provides a certain level of security, by coping with the malicious behaviors of some of the participants. As a blockchain maintains records of the ownership of digital assets, malicious users are incentivized to try to tamper with these records, to change ownership. It is thus crucial to have good ways to prevent such outcomes.

Validation element. Transactions are issued by users of a blockchain in order to transfer the ownership of digital assets. For example, Alice might issue a transaction T that transfers 1000 coins to Bob. To prevent a malicious user, say Carol, from withdrawing coins from Alice's account without her consent, Alice must digitally sign this transaction T.

There exist various methods to create the public and private key pairs of each client necessary for this asymmetric cryptographic system [8]. Secp256k1 [4] is used by Bitcoin and Ethereum but has been shown vulnerable to some attacks [3]. Some concerns exist regarding the security of elliptic curves standardized by the NIST 19 years ago [13], but more secure alternatives have recently been proposed and standardized by the IETF [11]. These standards should be applied to the blockchain standards to define the level of security that operators and service provider should offer to their users.

4.3 Onwership element

4.3.1 Transactions

As briefly mentioned a transaction comprises a set of information that indicates the transfer of digital assets between accounts. There exist multiple forms of transactions that have proved useful in practice. Bitcoin allows users to issue simple scripted transactions, also called Pay-To-Public-Key-Hash (or P2PKH for short) transactions, that pay Bitcoins to an account identified with the hash of its public key.

More sophisticated types of transactions can be defined within the Bitcoin scripting language and have also become popular in other cryptocurrencies. A prominent example is the multisignature (or multisig for short) transactions that allow the coin transfer under the condition that multiple signatures are provided.

These transactions work for a specific type of blockchain implementations, those compliant with the unspent transaction output (UTXO) model of Bitcoin. They express the balances of accounts as a series of UTXOs, meaning that the balance of account A is the sum of all the amounts transferred to A that have not been consumed. To execute a transfer from an account B to another account C, one has to consume some of the UTXOs corresponding to this account B and generate the corresponding UTXOs corresponding to account C.

The difficulty of interoperability of blockchain systems stems not only from their independent management of identities but also from the differing transaction formats. For example, in order to support other type or payments the Ethereum blockchain system uses a more elaborate scripting language and a completely different transaction model.

4.3.2 Smart contracts

A smart contract is a program that executes a series of actions depending on some conditions. It allows users to define how the transfer of digital assets can occur, depending on factors visible within the closed world of the blockchain's historical transactions. This can be more expressive than the Bitcoin scripting language, and may execute more complex business logic.

Programming languages. In order to support smart contracts, Ethereum [15] provides a Turing-complete virtual machine interpreter called the Ethereum Virtual Machine. Higher-level programming languages such as Solidity, can be used to write program that define ownership rules for custom digital assets.

There is a large variety of programming languages for writing smart contracts. For example, in Tezos, smart contracts can be written in the type-safe OCaml functional programming language. The increasing use of safer smart contract languages has been motivated by historical problems with code that has had unexpected behaviors. One of the prominent examples was when Ethereum suffered a re-entrancy bug in 2016 that malicious users exploited to repeatedly withdraw money and steal a total of AU$65 million worth of the cryptocurrency.

Each platform usually has its specific programming language, although there are some exceptions: Hyperledger aims at supporting go and other languages, like Java.

Legal aspects. Smart contracts are particularly interesting from a legal perspective. Smart contracts, as programs, can encode rules to automatically enforce or detect the violation of those rules. Those rules may be intended to encode provisions from contracts or legislation. However, there is still some work to be done to guarantee that implementation accurately captures the legal intent of the rules, and that the program is accurately converted by a compiler into a bytecode representation for execution by the blockchain virtual machines. These different layers introduce potential sources of ambiguities that are difficult to eradicate.

One approach is to develop technologies for formal verification of smart contracts [2]. Another approach is to automatically detect well-known bugs within smart contracts [9]. Because this is simpler than verifying the correctness of the program, it can be executed at runtime even before the smart contracts get stored within the blockchain.

Tokens. Smart contracts have been used to raise funds to support new business ideas. The process named Initial Coin Offering (ICO) allows a company to sell tokens in exchange for cryptocurrency. Depending on the business model, these tokens might represent partial ownership of a company or asset, or might represent the pre-purchase of a tradeable right to use a service.

In Ethereum, the ERC20 standard defines a series of rules that an Ethereum token contract must comply with.[11] These ERC20 tokens implement a series of functions that let Ethereum users trade tokens. ICOs have attracted a lot of funds without being subject to clear regulation. However, recently organizations like the U.S. Securities and Exchange Commission (SEC) have started to view most ICOs tokens as securities. These tokens would then be subject to the same regulations as other securities.

5 Conclusion

There have been many initiatives created internationally to work towards blockchain and DLT standardization. However, we are still at the beginning

[11] `https://theethereum.wiki/w/index.php/ERC20_Token_Standard`.

of understanding best practices for this rapidly changing technology.

We have proposed terms and highlighted potential confusions to outline how crucial it is to reach a consensus on the basic terminology. Implementing a blockchain requires knowledge from disciplines including distributed computing and cryptography. Terminology to describe the properties these implementations should meet is necessary not only for interoperability but also to express expected guarantees to their users.

The risk of standardizing an emerging technology too early is that it may limit the development and adoption of improved technology. Standards for terminology can reduce basic misunderstandings, but should be defined in a way that gives flexibility to support future innovation. Although the blockchain and DLT landscape is rapidly changing, we can still draw on existing technical knowledge from foundational disciplines. Even beyond pure technical foundations, existing approaches to regulation and governance may help us to define what can and cannot be expected from these services and what is the part of responsibility shared by users, operators and services providers.

Acknowledgments

This research is in part supported under Australian Research Council Discovery Projects funding scheme (project number 180104030) entitled “Taipan: A Blockchain with Democratic Consensus and Validated Contracts”.

References

[1] ISO/IEC 29100 - Information technology - Security techniques - Privacy framework. 2011-12-15. ISO/IEC 29100:2011.

[2] Sidney Amani, Myriam Bégel, Maksym Bortin, and Mark Staples. Towards Verifying Ethereum Smart Contract Bytecode in Isabelle/HOL Proceedings of the 7th ACM SIGPLAN International Conference on Certified Programs and Proofs, 66–77, 2018.

[3] Joppe W. Bos, J. Alex Halderman, Nadia Heninger, Jonathan Moore, Michael Naehrig, and Eric Wustrow. Elliptic Curve Cryptography in Practice. Technical report MSR-TR-2013-119, Nov. 1, 2013.

[4] Daniel R. L. Brown. Standards for Efficient Cryptography - SEC 2: Recommended Elliptic Curve Domain Parameters, Certicom Corp., Version 2.0, Jan. 27, 2010.

[5] Blockchain Consensus. Tyler Crain, Vincent Gramoli, Mikel Larrea, and Michel Raynal. 19 eme rencontres francophones sur les aspects algorithmiques de télécommunications (AlgoTel'17), 2017.

[6] Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, Nickolai Zeldovich. Algorand: Scaling Byzantine Agreements for Cryptocurrencies. SOSP 2017.

[7] Vincent Gramoli. The Red Belly Blockchain. Invited talk, MIT (MA), USA. July 2017.

[8] ISO/IEC 14888-3:2016. Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms. `https://www.iso.org/standard/64267.html`. March 2016.

[9] Anton Jurisevic, Lexi Brent, Eric Liu, Michael Kong, Francois Gauthier, Vincent Gramoli, Ralph Holz, Bernhard Scholz. A Scalable Bug Checking Framework for Smart Contracts. Unpublished technical report, 2018

[10] Lamport L., Shostack R., and Pease M., The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, 4(3)-382-401, 1982.

[11] Curve25519 - RFC7748 Elliptic Curves for Security, Section 4.1. A. Langley, M. Hamburg, S. Turner. Jan. 2016. `https://tools.ietf.org/html/rfc7748#section-4.1`

[12] Satoshi Nakamoto. Bitcoin: a peer-to-peer electronic cash system. 2008. `http://www.bitcoin.org`

[13] National Institute of Standards. Recommended Elliptic Curves for Federal Government Use. July 1999. `http://csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf`

[14] Vizier G., Gramoli V. ComChain: Bridging the Gap Between Public and Consortium Blockchains. IEEE Blockchain 2018.

[15] Gavin Wood. ETHEREUM: A Secure Decentralised Generalised Transaction Ledger. Yellow paper. 2015.

Vincent Gramoli (member of IEEE) is the head of the Concurrent Systems Research Group at the University of Sydney, a senior researcher at Data61-CSIRO and the Chair of the Blockchain Technical Committee at the Australian Computer Society. He obtained a PhD in Computer Science from Université de Rennes and an Habilitation in Computer Science from UPMC Sorbonne University. Prior to arriving in Australia, he was affiliated with INRIA, Cornell University, the Swiss Federal Institute of Technology Lausanne and NICTA among others. His research interest is in distributed computing including the fundamental issues of blockchain systems. With his research group, he designed the Red Belly Blockchain, a fast and secure blockchain system.

Mark Staples (member of IEEE) holds Bachelor of Information Technology (1992) and Bachelor of Science in computer science and cognitive science (1992) from the University of Queensland, and a PhD in computer science (1998) from the University of Cambridge. He is a Senior Principal Research Scientist at Data61 (CSIRO) in Sydney Australia, and is a Conjoint Associate Professor in the School of Computer Science and Engineering at UNSW. He has previously held roles in industry in software engineering and systems engineering management, in domains ranging from SCADA systems, electronic payments, and implantable active medical devices. His research is on software architecture, blockchain technologies, software engineering, and philosophy of engineering. He is on the Standards Australia committee IT-041 and ISO committee TC307 for standardization of blockchain and distributed ledger technology.