GEDE - Assertions on Blockchain Technology

Editors: Wolfgang Kuchinke, Peter Wittenburg

State: November 2018

In this 1st Version we collect simply all kinds of relevant statements made on Blockchain Technology (BCT), independent whether we support the individual statements or not. There are so many documents out there that we need to be selective in what to include. Most of the documents are just PR statements to get a share of the market or funding - not worth spending time on it. In a second step we will cluster and comment on the statements. In a third step we will write a coherent report summarising the conclusions.

### 1. NIST Assertions

The NIST document is an extensive and careful analysis of the BCT and discusses possible use cases. Here we can only mention a few summarising statements. We recommend reading that document.

1. BC are tamper evident and tamper resistant digital ledgers implemented in a distributed fashion and usually without central authority. They enable a community of users to record transactions in a shared ledger within that community without the chance to change transactions later.
2. In Bitcoin users can digitally sign and transfer rights to that information to another user and all participants can independently verify the transaction's validity. Bitcoin BC is stored, maintained, and collaboratively managed by a distributed group of participants.
3. There is hype around BC without understanding the technology in detail. There is a tendency to want to apply it to every sector in every way imaginable.
4. There are many different models in the way to reach consensus about validity of transactions and about how to create a new block to embed the transaction. And there is one big distinction about the nature of the community: In permissionless BC networks anyone can read and write to the blockchain without authorisaton. Permissioned BC networks limit participation to specific people and organisations and allow finer-grained controls.
5. In BCs there is one common ground: each block is comprised of a block header with metadata about the block and a body containing transactions. Every block header contains a cryptographic link to the previous block's header.

### 2. Dutch Blockchain Coalition: Thematic Report Blockchain and the GDPR

1. GDPR compliance is not about the technology, it is about how the technology is used. Just like there is no Gdpr-compliant Internet, or GDPR-compliant artificial intelligence algorithm, there is no such thing as a GDPR-compliant blockchain technology. There are only GDPR-compliant use cases and applications. Among other things, in this report we observe that many of the Gdpr’s requirements are easier and simpler to interpret and implement in private, permissioned blockchain networks than in public, permissionless networks.
2. The tensions between Gdpr and blockchain revolve mainly around three issues:
   * The identification and obligations of data controllers and processors. While there are many situations where data controllers and data processors can be identified and comply with their obligations, there are also cases where it is difficult, and perhaps impossible, to identify a data controller, particularly when blockchain transactions are written by the data subjects themselves.
   * The anonymisation of personal data. There are intense debates, and currently no consensus, on what it takes to anonymise personal data to the point where the resulting output can potentially be stored in a blockchain network. To take one example, the hashing of data cannot be considered to be an anonymisation technique in many situations, and yet there are cases where the use of hashing to generate unique digital signatures of data that is stored off-chain, is potentially conceivable on a blockchain.
   * The exercise of some data subject rights. We note that if personal data is recorded in a blockchain network, it may be difficult to rectify or remove it. Defining what can be considered erasure in the context of blockchains is under discussion.
   * To be clear, these issues have not been conclusively settled by the data protection authorities, the European Data Protection Board (EDPB) or in court.
3. Meanwhile, we propose Four rule-of-thumb principles that entrepreneurs and innovators can consider:
   * Start with the big picture: how is user value created, how is data used and do you really need blockchain?
   * Avoid storing personal data on a blockchain. make full use of data obfuscation, ncryption and aggregation techniques in order to anonymise data.
   * Collect personal data off-chain or, if the blockchain can’t be avoided, on private, permissioned blockchain networks. Consider personal data carefully when connecting private blockchains with public ones.
   * Continue to innovate, and be as clear and transparent as possible with users.
4. Blockchain technology is new and complex to understand. Additionally, it is still immature and it should not be surprising to citizens and regulators that not every ‘t’ has been crossed.

### 3. V. Vallivaara Assertions

#### 3.1 Can BC help Changing the Data Culture

1. BC is a cryptographically protected distributed register of confirmed transactions or contracts. Ledger contains of blocks with transactions that are connected through hash chaining and that are shared in near real-time.
2. Smart Contracts are special transactions enabled in Ethereum, Hyperledger etc. They include pre-written logic also stored and replicated in BCs and are triggered automatically under defined conditions.
3. Data are tradeable goods and should have clear identities as required by Digital Objects. Combining DOs with smart contracts would give the possibility to safely document all transactions. Changes in DO's ownership are safely stored as transactions in BC. SC include the access control specs, use conditions etc.

#### 3.2 BCT and New IoT Challenges

1. In the absence of a legal framework around Smart Contracts, it is uncertain who is liable for what if there is a failure of any sort. Code can't be law and the technology owners don't have a formal position.
2. The DAO Ethereum case is analysed and indicates a possible attack.

### 4. Blockchains and IoT: a reality check

**P. Nikander (Aalto u)**

1. A full node for Distributed Ledger technology is bulky, but needed to establish trust and trust involves careful checking.
2. Setting up an Ethereum archival node storing all Ethereum history requires 1.1 TB of striped SSD, a server class host and even using Finlands fastest network costs about 2 weeks.
3. Setting up an Ethereum full node that is able to verify new transactions and mine new ones requires 2 hours. The time it takes to secure a transaction costs about 2 minutes and thus about 1 $.
4. DLTdoes not help individual IoT systems, trusted nodes are required. DLT are not a panacea for IoT security challenges, since public DLTs are very expensive in use (cost of computing in Ethereum about 1 Mio times higher than computing in cloud)

### 5. K. Jeffery's Assertions

Articles are appearing with the following criticisms:

1. It is expensive on computing power and networking capacity;
2. Lack of regulation makes it a risky environment (especially for cryptocurrencies of course);
3. It is complex to understand; the complexity was designed to overcome the problems of the 2018 financial crash but is the complexity still necessary;
4. The technology is slow and cumbersome compared with traditional database technology;
5. There is resistance from ‘the establishment’ and so take-up in mainstream IT has been very slow (~20 years already; the WWW took off in just a few years);
6. It has proprietary interfaces – no open standards – which contrasts with the claimed transparency of the technology;
7. There are some interesting start-up companies trying to utilise ad improve blockchain technology – especially outside of the cryptocurrencies environment.
8. ERCIM News has an interesting summary of statements on BCT: <https://ercim-news.ercim.eu/en110/> . In the following some ERCIM descriptions are included since they give a good overview about various activities wrt BCT.

#### 5.1 ERCIM: Introduction to the Special Theme BC Engineering

**E. Andoulaki (IBM), M. Jarke (RWTH, FIT), J-J. Quisquater (Leuven)**

1. BC can be understood as distributed ledgers combining transparent and falsification proof documentation with distributed trust.
2. Scalability, anonymity, security and durability are ensured by distributed storage combined with cryptographic primitives and protocols.

#### 5.2 ERCIM: BC for Everybody

**J-J. Quisquater (Leuven)**

1. Trust, transparency and traceability are important in online transactions. Creating a permanent trace is essential.
2. Coordinated time stamping is also required in many cases (patents, etc.)
3. Smart contracts is a promising new idea enabling complex internal verifications to avoid problems.
4. Current challenges are: scalability, latency in registration, merging of blockchains, renew BC in case of errors, handle the right of forgotten. Quantum computers may solve the computational needs.
5. With BC we are still at the stage of experiments, not of fully ready products.

#### 5.3 ERCIM: Permissioned BC and Hyperledger Fabric

**E. Andoulaki et al (IBM)**

1. BC are immutable decentralised ledgers for recording transactions that are to various degrees resilient to malicious behaviour. Ledger consists of blocks (groups of transactions) linked together in a hash-chain establishing a total order among blocks and transactions.
2. Smart contracts are application that operate on top of blockchains with guaranteed execution consistency across distributed peers.
3. Permission-less BC are open and anybody can participate without having a specific identity. Permissioned BC are an alternative to open BC, since only known and identifiable are accepted in the BC network, eventually not fully trusted.
4. Permissioned BC can be designed to meet certain performance, scalability and cryptographic standards.
5. IBM Hyperledger Fabric is a framework for executing distributed applications in untrusted environments executing smart contracts.

#### 5.4 ERCIM: Bitcoin - Cryptocurrencies and Alternative Applications

**A. Judmayer et al (SBA Research)**

1. Bitcoin introduced the proof-of-work (PoW) randomised consensus approach working with an unknown number of participants in permission-less networks.
2. 22% of Bitcoin users experienced monetary loss (lost bitcoins) due to security breaches and self-induced errors. Nevertheless, more than 650 different cryptocurrencies are in circulation. The security of BC in a multi-PoW blockchain world has not yet been sufficiently studied.
3. If not enough honest miners (nodes capable to generate blocks) or mining pools join new cryptocurrencies at the start phase, the latter becomes vulnerable to dishonest miners. Techniques for improvements of security are being studied.
4. In current PoW based BC (Bitcoin) there is a trend that nodes (miners) with much computer power get a preference in creating new blocks, i.e. there is a bias in mining affecting the ecosystem in a non-intended manner.

#### 5.5 ERCIM: Identity Management on the BC

**D. Augot (INRIA) et al**

1. Participation in Bitcoin like permission-less BC networks is anonymous. Proposed is a technique to obtain assured identities based on face-to-face proofing but hiding the identity to the rest of the network, but nevertheless being able to use these BC identities to access services.
2. BC can be used to store such identities in form of crypto-certificates and there is a trusted instance that knows about the identity.
3. This can help to overcome one of the great obstacles in permission-less networks.

#### 5.6 ERCIM: SpaceMint: A Cryptoccurency Based on Proofs of Space

**G. Fuchsbauer (INRIA)**

1. SpaceMint is a cryptocurency that replaces energy-intensive computation underlying most of today's systems by replacing "proof of work" by the "proof of space" concept.
2. Bitcoin-like BC waste enormous amounts of electricity and have a tendency to concentrate control in the hands of a few nodes with much computational capacity - the costs to participate as "miner" are extremely high. The chances of mining (creating) the next block are proportional to the miner's invested computation which results in a rewarding of freshly minted (created) coins.
3. PoW has some implications such as limited block size limiting scalability, questions about long-term stability and sustainability.
4. Proof of Stake is an alternative where the chance of creating the next block is proportional to the amount of currency held by the miner. Since mining is cheap PoStake is subject of attacks and a large number of currency holders must be online and mine to make it functioning well.
5. In Proof of Space, miners need to invest in disk space and the size influences the chance to create a new block. The advantage is that the disk capacity can be used for other purposes, while in PoW CPU capacity is simply burnt due to the mining process.

#### 5.7 ERCIM: Coinblesk - A realtime, Bitcoin-based Payment Approach

**T. Bocek (U Zürich) et al**

1. BC implicitly pave the path towards secure data storage in a decentralised manner. Smart contracts make them interesting for many use cases. SC are formalised protocols to facilitate, verify, and enforce the negotiation or performance of a contract.
2. CoinBlesk is an App which includes a Bitcoin payment server where sellers and buyers are able to handle Bitcoin payments. Transactions are batched (aggregated), then signed by the signature of the client and then sent to the BC network to reduce the costs per transaction which has to do with the inefficiencies of BCT. The user can specify how big the batches to be signed should be.
3. The system only works if all users can be sure that the payment server does not disappear or if a refunding option is given.

#### 5.8 ERCIM: Bitcoin Unchained

**C. Carr (NTNU) et al**

1. Bitcoin BC causes incompressible transaction delays and incentivises consolidation of mining power. Bitcoin miners compete for creating new blocks and get rewarded by new coins. (current fees for transactions are 10 $).
2. They are working on a technology to remove the block concept. Instead when a transaction is to be made, creators simply reference two recent existing transactions. The collection of recent previous transactions is rewarded. By removing blocks the large confirmation delay due to the PoW algorithms is removed.

#### 5.9 ERCIM: A holistic Approach to Smart Contract Security

N. Stifter et al (SBA Research)

1. SC form a computerised transaction protocol that executes the terms of a contract. A BC based SC platform serves as a decentralised arbiter to both verify and enforce the execution of these SCs based on the platform's defined rules. It is about trusted computing (of certified code) with a high trust in a decentralised environment.
2. Bitcoins only offers very limited SC functionality to ensure correctness. Other platforms (Ethereum, etc.) offer support "complex and stateful Turing-complete" contracts allowing a wider spectrum of applications. The correct and secure execution of such SC depends on the SC code, its execution environment and in particular properties of the distributed system requiring a holistic view. Serious incidents have been recognised where the setup failed.
3. An agenda of aspects to be analysed in future is presented.

#### 5.10 ERCIM: Correctness of SC for Consistency Enforcement

**T. Osterland, T. Rose (FIT)**

1. SC are a mechanism to help maintain consistency among data and transactions and are automatically triggered by the conduct of a transaction. They enable a full automation of agreements and the autonomous adherence to these agreements.
2. Participation in Smart Energy Grids requires a permission-less and self-regulating approach. There is no need for a central control and for trusting each other. And big companies can be treated like small suppliers.
3. All bookkeeping and payment exchange could be handled by SC, there is 24/7 uptime and decentralisation protects against catastrophes and terrorism acts. However, a certification of all code needs to take place before entering the BC which is not a trivial task for complex applications.

#### 5.11 ERCIM: Implementation of a BC Workflow Management Prototype

G. Fridgen (FIT) et al

1. Intercompany workflow management is seen as a promising application area. A BC prototype is in development to document a joint letter of credit in international shipping. Achieving transparency and traceability is currently a cumbersome manual process involving many actors. Much paper needs to be sent currently and many signatures need to be collected with lots of delays between asynchronously working people.
2. BC could be used to document that papers have been signed and are available to everyone without delays based on secure mechanisms. Dealing with credits fully digitally is an application for BCT, in particular since parallel processes can be started reducing delays.
3. Yet this is just a test due to the early stage of the BCT and lacking appropriate legislation.

#### 5.12 ERCIM: Proofs of Work - the Engine of Trust

**A. Biryakov (U Lux)**

1. Due to the functioning of PoW, short after introduction of Bitcoin the mining process entered into an arms race of mining hardware. Bitcoin mining is currently in the hands of about a dozen mining farm operators. However, this mining centralisation is against the original decentralisation ideas.
2. The challenge is therefore to design more democratic mechanisms such as Proof of Stakee, etc. which also can reduce the gigantic waste of energy (currently Bitcoin burns energy comparable to a country such as Denmark).

#### 5.13 ERCIM: Design Requirements for a Branched BC Merging Algorithm

**A. Melissen (Storro bv)**

1. In standard BCT branching of chains is both implicit and inevitable. Bitcoin, dependent on fast consistency proof, has an effective mechanism for branch selection/merging, however, limits the network practically to one branch and thus introducing a scaling bottleneck.
2. Finding more optimal merging algorithms for these distributed BC preserving is still a subject of research.

#### 5.14 ERCIM: Blockchain – Attack on and Chance for the Public Sector

**C. Welzel (FOCUS)**

1. Often the state and the public administration act as intermediary to regulate and oversee transactions. Therefore, several registries are maintained to manage ownership etc.
2. A technology such as BC replacing intermediaries is of natural interest for this sector.
3. Estonia is active to use BCT to provide notary services and for a Keyless Signature infrastructure with the expectations to create more effective solutions.
4. Also in Dubai BCT is being tested with goal to process all government documents to increase transparency.
5. No clear results are presented, but vague recommendations: monitor BCT, build test cases, push standardisation, actively shape the use of BCT.

#### 5.15 ERCIM: How distributed ledgers can transform healthcare applications

**A. lo Duca et al (IIT CNR)**

1. The domain of healthcare documents is scattered making it impossible to create a merged history of a personal health record, i.e. actors do not have access to the full record.
2. A solution is recommended where the store of all patient records are separated from the database that specifies how to access the records. A distributed Data Lake is constructed that contains all personal health records - (obviously still a local copy maintained in the hospitals). The Distributed Ledger (DL) stores all pointers to the records in a secure way. Via public/private key methods and fine-tuned access control policies regulated for example by smart contracts secure access can be given to the information in the DL about the health records.