Analysis of Blockchain Use Cases in the Citizens Broadband Radio Service Spectrum Sharing Concept

Seppo Yrjölä(✉)

Nokia Innovation Steering, Oulu, Finland
seppo.yrjola@nokia.com

Abstract. The Blockchain (BC) technology has received religious attention in the financial and internet domains, and recently interest has spread to adjacent sectors like communications. This paper seeks to identify the impact of the BC technology in novel spectrum sharing concepts using the Citizens Broadband Radio Service (CBRS) concept as an example. The results indicate that the BC core characteristics can be utilized in several use cases addressing current CBRS implementation considerations. The CBRS concept could particularly benefit of BCs in building trust, consensus and lowering the transaction cost. In BC deployments, confidentiality should be taken into consideration through hybrid and private BC options. Furthermore, the cognitive radio spectrum sharing – BC combination paves the way for new business models and distributed services.

Keywords: Blockchain · Citizens Broadband Radio Service · Cognitive radio Mobile broadband · Spectrum sharing · 5G

1 Introduction

The number of mobile broadband (MBB) subscribers, connected 'things' and the amount of data used per user is set to grow significantly leading to increasing spectrum demand [1]. The US President's Council of Advanced Science & Technology (PCAST) report [2] emphasized the need for novel thinking within wireless industry to meet the growing spectrum crisis in spectrum allocation, utilization and management. The essential role of cognitive radio and spectrum sharing were underlined to find a balance between the different services with their different spectrum requirements and system dynamics. At the same time, Blockchain (BC) technology has received significant attention as a potential answer to the most vexing trust and data security challenges related to transactions, contracting, and funds exchange in the Internet across various domains [3]: from original bitcoins [4] and finance [5], to real estate [6], health [7], energy [8], and government [9]. In telecommunications, to date early BC studies has focused mainly on the context of Internet of Things (IoT) [10].

So far, only a subset of the cognitive radio (CR) [11] and spectrum sharing concepts researched in technology and regulation has reached market acceptance, the license exempt access with intelligent user terminals and spectrum sensing [12], Dynamic Spectrum Sharing (DSA) non-collaborative concept with radar detection

P. Marques et al. (Eds.): CROWNCOM 2017, LNICST 228, pp. 128–139, 2018.
https://doi.org/10.1007/978-3-319-76207-4_11

function of Dynamic Frequency Selection (DFS) [13], or the unlicensed TV White Space (TVWS) [14, 15] as examples. Based on the decade of profound CR and in particular TVWS concept studies, a couple of novel licensing based sharing models have recently emerged, and are under regulation and standardization, the Licensed Shared Access (LSA) [16] from Europe and the Citizens Broadband Radio Service (CBRS) from the US [17]. Related to these prominent spectrum sharing concepts, particularly for the CBRS, there is not prior research regarding their business and technology enabler analysis. Market success criteria for dynamic spectrum access technologies in general has been studied in [18], and the feasibility and attractiveness of the CBRS spectrum sharing concepts applying business model theory framework has been addressed in [19]. In [20], different CBRS stakeholder groups' considerations are summarized and general Spectrum Access System (SAS) requirements discussed. Moreover, the applicability and validation of the Internet and MBB technology enablers has received very little attention as focus to date has been on more general and future oriented CR techniques [21]. In the literature, to the best knowledge of the author, no research to date has analyzed the application of the BC technology and its underlying characteristics to the spectrum sharing concepts. This paper investigates:

1. What kind of blockchain characteristics support spectrum sharing concepts and the CBRS framework?
2. What are the potential use cases?

The rest of the paper is organized as follows. First, the CBRS framework and the BC technology are shortly introduced in Sects. 2 and 3. Section 4 links CBRS deployment considerations with the BC technology characteristics into potential use cases, and analyze their applicability. Conclusions are drawn in Sect. 5.

2 Citizens Broadband Radio Service Concept

The Federal Communications Commission (FCC) released Report and Order and Second Further Notice of Proposed Rulemaking to establish rules for shared use of the 3550–3650 MHz band in April 2015 [17]. Followed by intense discussion and consultation with the industry [22], the FCC released second Report and Order and Order on Reconsideration [23], and finalizes the rules [24] governing the CBRS in the 3550–3700 MHz band in 2016. The framework defines a contiguous 150 MHz block that the FCC calls *Citizens Broadband Radio Service*. The 3550–3650 MHz spectrum is currently allocated for use by the US Department of Defense (DoD) radar systems and Fixed Satellite Services (FSS) while the 3650–3700 MHz spectrum incumbents are the FSS and the grandfathered commercial Wireless Broadband Services (WBS). The FCC prefigures the CBRS as an "innovation band" where they can assign spectrum to commercial MBB systems like the Third Generation Partnership Project (3GPP) Long Term Evolution (LTE) on a shared basis with incumbent users.

The sharing framework consists of three tiers: *Incumbent Access* (IA), *Priority Access* (PA) and *General Authorized Access* (GAA). The FCC licenses for the PA layer users will be assigned via competitive bidding, and allowed to operate up to a total of 70 MHz of the 3550–3650 MHz spectrum segment enjoying interference protection from the GAA operations. A *PA License* (PAL) licensee's non-renewable authorization is for a 10 MHz channel in a single census tract for three years, with the ability to aggregate up to six years up-front. One licensee may hold up to 40 MHz of PALs in any given census tract at any given time. In addition to MNO and WBS users the PAL layer may cover utilities, IoT verticals and governmental users. The specific channels of auctioned PALs are assigned, re-assigned, and terminated by the *Spectrum Access System*. The PALs will be opened for the third GAA tier users, when unused and further automatically terminated and may not be renewed at the end of the term. The '*use*' status of PALs in the CBRS 'use it or share it' approach is determined using two engineering approaches [23]. First, licensees should report the coverage area of the set of *CBRS devices* (CBSDs) based on actual network deployments called the *PAL protection area* (PPAs). Second, to maximize an objective PPA, the SAS maintains a list of CBSDs belonging to the PPA and do not authorize other CBSDs on the same channel in geographic areas and at maximum power levels that will cause aggregate interference within a PPA [23].

The FCC revisited the CBRS rules [24] in 2016, and introduced the *light-touch leasing process* to enable secondary markets for the spectrum use rights held by PA licensees. Under the framework, no FCC oversight is required for partitioning and disaggregation, and PA licensees are free to lease any portion of their spectrum or license outside of their PPA. The PPA can be self-reported by PAL owner or calculated by the SAS. The PAL channel can be re-allocated beyond the PPA, but within the census tract. Furthermore, the FCC will permit stand-alone or SAS managed *spectrum exchanges* and let market forces determine the role of the SAS value added services.

The opportunistic GAA operates under a *licensed-by-rule* framework and has no interference protection from other CBRS users, while it must protect incumbents and PALs. This dynamic third layer with the minimum availability of 80 MHz aims to facilitate the rapid deployment of compliant small cell devices while minimizing administrative costs and burdens on the public, licensees, and the FCC. Furthermore, the GAA is planned to spur innovation as a flexible and scalable low-cost entry point for a wide choice of services and new entrants, e.g., small and local businesses, utilities, healthcare, public safety and smart cities. For established Mobile Network Operators (MNOs) and PAL licensees, the GAA offers, e.g., PAL offload during IA interruption, Wireless local access network (Wi-Fi) type capacity offload, backhauling and WBS.

The CBSDs are fixed base stations (BS), or networks of such, and can only operate under the authority and management of a centralized SAS, which could be multiple as shown in Fig. 1. Both the PAL and the GAA users are obligated to use only the certified FCC approved CBSDs, which must register with the SAS with information required by the rules, e.g., operator ID, device identification and parameters, and location information. In a typical MNO deployment scenario, the CBSD network is a managed network comprising of the *Domain Proxy* (DP) and Network Management System (NMS) functionality. The DP may be a bidirectional information routing engine or a more intelligent mediation function enabling flexible self-control and interference optimizations in such a network. In addition, DP enables combining, e.g., the small cells of a shopping mall or sports venue to a virtual BS entity, or provides a translational capability to interface legacy radio equipment with a SAS.

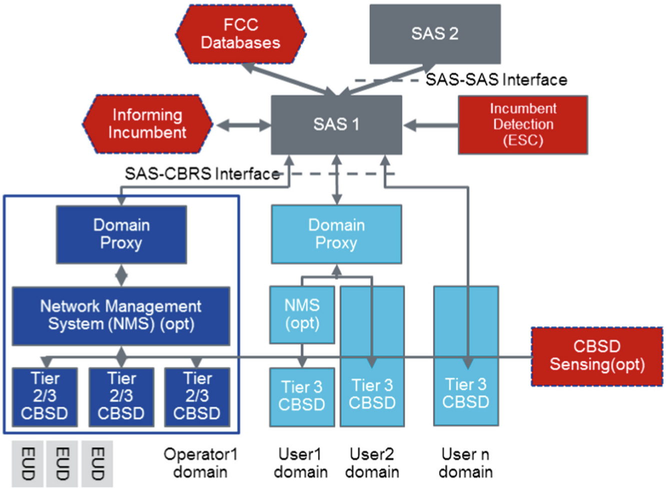

Fig. 1. CBRS functional architecture.

In addition to spectrum assignment, the SAS controls the interference environment, and enforces protection criteria and exclusion zones to protect higher priority users, and dynamically determines and enforces CBSDs maximum power levels in space and time [23]. In the recent FCC rules [24], the FCC requires all SASs to have consistent models for interference calculations. Furthermore, the SAS takes care of registration, authentication and identification of user information, SAS-SAS message exchange, and performs other functions as set forth in the FCC rules [20]. All the CBSDs and End User Devices (EUDs) must be capable of two-way communications across the entire 3.5 GHz band and discontinuing operation or changing frequencies at the direction of the SAS. In order to meet the mission critical requirements of the DoD IAs, the FCC adopted rules to require *Environmental Sensing Capabilities* (ESC) in and adjacent to the CBRS band to detect incumbent radar activity in coastal areas and near inland military bases. The confidentiality of the sensitive military incumbent information will be ensured through strict operational security (OPSEC) requirements and corresponding certification for the ESC elements and operator authorization [25]. Once IA activity is detected, the ESC communicates that information to a SAS for processing, and if needed, a SAS orders commercial users to vacate an interfering channel within 300 s in frequency, location, or time [23].

The CBRS market introduction is planned to start with the opportunistic GAA layer and incumbent protection utilizing static *exclusion zones* (EZ) only to provide a low-cost entry point into the band. In the second phase, the ESC system enables the rest of the country, particularly major coastal areas to become available, as the EZs will be converted into *protection zones* (PZ). ESC deployments near the EZs can consist of commercially operated sensor networks, or CBSD infrastructure based sensing or their combination. Prospective SAS administrator with ESC or stand-alone ESC operators must have their systems approved through the same process as SAS administrators.

The *FCC databases* are in authority to input the FCC information, e.g., registered or licensed commercial users, EZ areas requiring ESC into SAS. Additionally, the functional architecture depicted in Fig. 1 includes the *Informing Incumbent* option enabling the federal IA to directly inform the SAS ahead of plans concerning changes in the spectrum usage [26].

The Spectrum Sharing Committee (SSC) of the Wireless Innovation Forum (WInnF) [27] consisting of governmental, MBB, wireless, Internet and defense ecosystems representatives has finalized operational and functional requirements protocols for data and communications across the various open interfaces within the system [27] to enable early trial implementations of interoperable systems. The White House aims to expand wireless innovation in spectrum sharing further through identifying an additional federal owned spectrum for future commercial sharing, subject to the success of sharing at 3.5 GHz [28].

3 Blockchain Technology

In 2008, Nakamoto [4] outlined a new bitcoin protocol for a P2P electronic cash system using cryptocurrency, i.e., a digital or virtual currency that uses cryptography for security. This protocol introduced a set of rules in the form of decentralized, distributed processes that ensured the integrity of data exchanged among numerous non-trusting participants without going through a trusted central intermediary. Blockchain can be defined as a digital ledger designed to keep a transparent, accessible, verifiable and auditable distributed record of data sets tagged from different pieces of information belonging to different participants. Furthermore, BC networks can identify multi-entity conflicts, and forks and resolve them automatically to converge to a single, accepted view of events [29]. Figure 2 illustrates the typical steps in creating a BC [30] conforming the following general principles [3, 31]:

- Cryptography and hashing values validate data recorded on the BC and uniquely identify parties in a transaction. Blocks are encrypted in cascade, where the hash of the previous block will be used in the encryption of the current block.
- Each data item in a BC will have a timestamp, and confirmed ownership.
- Decentralized, distributed ledgers provide exact copies of transactions, which are shared by many parties in a P2P network.
- The choice of mining node, which broadcasts collected and validated block back to the network, depends on the consensus mechanism used.
- If the ledger of a BC tracks an asset, the ledger can be used to issue digital currency and perform financial transactions in that currency.
- BC publicly record digital transaction, though not with all the details. E.g., in many cryptocurrency ledgers and transaction platforms blocks are encrypted but transactions remain open.
- Private permissioned network option enables controlled, regulated environment with higher throughput compared to public type.

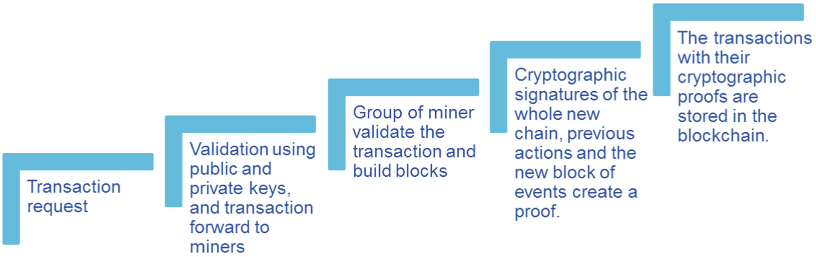
Transaction request
Validation using public and private keys, and transaction forward to miners
Group of miner validate the transaction and build blocks
Cryptographic signatures of the whole new chain, previous actions and the new block of events create a proof.
The transactions with their cryptographic proofs are stored in the blockchain.

Fig. 2. Illustrative blockchain process.

Blockchains have been outlined in [3, 31] to offer reduced transaction costs, improve security, open up new business opportunities, and transform existing value chains and business models. Particularly, the BC technology enables automatization and acceleration of business-to-business smart contracts and needed workflows implemented as a robust, distributed P2P system that is tolerant of node failures. A Smart contract is a computer code that is stored on a BC and runs in every node of the peer-to-peer network providing digitally signed, computable agreement between two or more parties [32]. It codifies and controls negotiation principles required in contracting like consensus, provenance, immutability and finality.

In parallel to research activities, established IT vendors and numerous startups are exploring BC opportunities across industries [30]. Recently, the Linux foundation announced the Hyperledger project [33], a collaborative effort to advance BC technology by identifying and addressing important features for a cross-industry open source ‘enterprise grade’ standard for distributed ledgers. Furthermore, Ethereum [34] has shown a proof of concept of the BC programming and smart contract platform.

Potential deployment considerations found in research and early trials, particularly in the financial sector, include throughput, scalability and latency in large public BCs, legal enforceability, transactional confidentiality particularly in the public BCs, consensus mechanism determination & complexity, and integration with legacy systems and workflows [10]. In a fully transparent public permissionless BC, every node independently verify and process all the transaction with full visibility into database’s current state, modification requested by a transaction, and a digital signature proving the origin. Furthermore, several discussed BC features were originally introduced in order to avoid regulatory restriction and enforcement. Regarding vulnerability and security concerns, BC technology has already been subject to one of the most aggressive environment by way of the Bitcoin cryptocurrency. In addition to technical consideration, particularly in the smart contract use cases the true issues were found in human centric legal and regulatory environment and processes [35]. The BC governance is a critical factor in the mitigation of the above-discussed issues. Hybrid and private BC options enable controlled consensus model environment with higher throughput and scalability compared to public type. Furthermore, white list of permitted miners with all blocks signed digitally by their miner of origin combined with distributed non-incentivized consensus scheme will significantly lower transaction costs.

4 Analysis of Blockchain Use Cases in CBRS

This section summarizes current implementation considerations with the CBRS concept, defines core characteristics of the BC, and develops potential use cases. The applicability of use cases are analyzed and assessed against BC core characterizes.

4.1 CBRS Implementation Considerations

Building on the definition of the CBRS and the BC, the following layers and interfaces in the functional CBRS architecture, depicted in Fig. 1, were identified as potential early adoption areas of the BC:

- Incumbent access system - that need to be protected while offering excess spectrum for sharing;
- National regulatory authority - conditions, rules and incentives for sharing;
- Spectrum Access System - database that stores the rules and availability of spectrum, spectrum assignment & interference control and spectrum broker;
- Environmental Sensing Capability - to detect incumbent activity while ensuring confidentiality;
- CBSD access networks - to utilize the PAL and the GAA spectrum, including optional DP and NMS;
- SAS - SAS communication - to exchange inter-SAS data records known to one SAS and communicated to another SAS;
- ESC - SAS interface - communicates information about the presence of a signal from a federal incumbent user system to one or more approved SASs.

In the early spectrum sharing research [12, 19–21] the following considerations and issues from technology, regulation, and business perspectives have been raised:

How to avoid lengthy and costly contractual agreements in a relatively short-term spectrum transaction while meeting regulatory reporting, tracking, and transparency requirements? In addition to the availability, liquidity and predictability of the shared spectrum it is essential to enable acceptably low incentifying ‘pay as you grow’ *transaction costs* for local small cell operators [18, 20].

How to ensure *integrity* of systems, network and shared cross-industry data? Particular consideration should be given to *OPSEC*, mission critical sensitive military incumbent data, and the operator’s *business sensitive* network data.

How to deploy inter-organizational near real time data and spectrum *asset exchange* between non-trusting *co-opetitive* stakeholders?

How to fully utilize sharing concept enabled unbundling of spectrum, infrastructure and services in *business model innovations*, e.g., through platform enabled as-a-Service business models for SAS and ESC and administrators, communication service providers, and technology vendors.

How to cope with growing data volumes and *complexity* while ensuring *scalability*? Dynamic channel assignment and co-existence management (CXM) of CBSDs becomes complicated due to a large number of small networks and standalone CBSDs in the same local geographical area, utilizing different radio technologies.

4.2 BC Core Characteristics

The applicability of the use cases can be analyzed against the following BC core characteristics discussed in Sect. 3 that differentiates it from the traditional relational database solutions:

1. Shared database write access with multiple writers;
2. Absence of trust between multiple writers;
3. Disintermediation;
4. Interaction and dependence between transactions (Fig. 3).

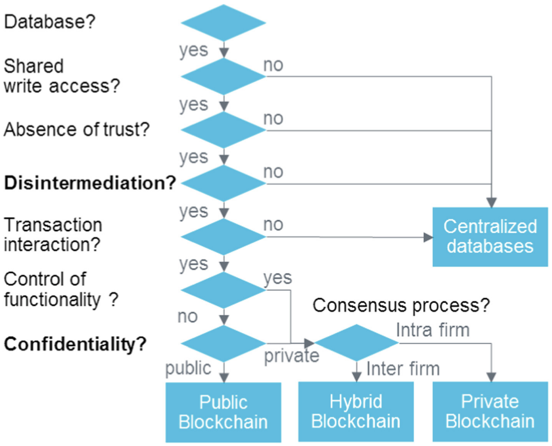

Fig. 3. Blockchain core characteristics and logic used in use case assessment.

Furthermore, *control of functionality, consensus process & validators*, and *confidentiality* factors will be used in analyzing the applicability of the public, hybrid or private BC options. In summary, considering trade-off in which disintermediation is gained at the cost of confidentiality.

4.3 Use Case Analysis

Based on the introduced BC characterization and early learning from the financial sector, BC use cases can be categorized in the following classes [36]:

- In *lightweight transaction*, one or more scarce assets are transacted and exchanged between limited numbers of participants utilizing a BC shared ledger marketplace.
- *Provenance tracking* tracks the origin and movement of high value items and assets across a supply chain utilizing virtual “certificates of authenticity”.
- In *inter-organizational recordkeeping*, BC acts as an authoritative final “transaction log” mechanism for collectively recording and notarizing any type of data of high importance or financial meaning.
- In *multiparty integration*, multiple parties write data to a collectively managed record in order to overcome friction while proving redundancy.

Lightweight transaction - Lower transaction cost and friction with resiliency and automatic reconciliation in real time can provide benefits in PAL spectrum Secondary Market Leasing Agreement (SMLA) *marketplace*, and ESC *sensor data as-a-Service* type of use cases [27]. Furthermore, BC could be used by the regulatory BC agent to inspect and record the data, and stop transaction if needed. In the future, deployments in dense urban areas and IoT verticals with similar types of needs for sharing could benefit of a common micro transaction marketplace. Additionally, inter-operator *roaming* connecting CBRS network users seamlessly to a 'coverage' networks can benefit of hybrid BCs with permissioned and public components eliminating third-party clearinghouses through smart contracts. The *neutral host* use case utilizes necessary resources in a specific geographic area, e.g., a building, campus or a public space like a sports stadium; manages these resources subject to agreements with resource owners and clients; and provides connectivity for clients to make use of the platform(s) to provide services to their end customers. Rules and agreements between the various asset providing networks can be codes as smart contracts.

Provenance tracking - CBRS applications can include common FCC ruled SAS interference calculation *models*, propagation models, elevation models and other associated geographic data, *product* (ESC, SAS, CBSD) centric system tests and certification, and integrity checking (e.g., supply chain tracking for OPSEC) for regulatory certification and periodic review and modification. In general, BC can be used to provide *Identity-as-a-Service* eSIM solution to machines in IoT environments.

Inter-organizational recordkeeping - *Audit trail* of critical communication with time stamps and proof of origin can be used in the FCC database, inter-SAS and ESC-SAS *data exchanges*, CBSD interference measurement data reporting. ESC performance monitoring and fault detection data [27], and for the *official registry* for government licensed assets and certified network elements, e.g., CBSDs. FCC OPSEC mitigation rules [24] on information gathering and retention withdraws ESC data from the potential BC use case list.

In *multiparty integration* - In the CBRS concept, elements and organization need a shared view of the reality, not originating from a single source. The *inter-SAS communication* (ISC) Essential Data [24] that shall be exchanged near real time symmetrically between all pairs of SASs consists of ESC sensor characteristics, CBSD physical installation parameters, CBSD coexistence parameters, information on all active CBSD grants, PPA records, and SAS-SAS coordination event records. In the future, collaboration can be extended to *co-existence management* (CXM) clearinghouse databases for exchange of co-existence related information, and inter-operator horizontal sharing. SASs with overlapping areas or operation must be capable of maintaining a consistent representation of the spectrum environment in order to maintain aggregated interference protection limits, avoid conflicting channel & spectrum grants, and to coordinate operations of all CBSDs in the CBRS band. Furthermore, CB smart contracts can be leveraged in inter-SAS data use agreements (Table 1).

Table 1. Summary of use cases and blockchain applicability analysis.

Use case	Shared write	Absence of trust	Disintermediation	Interaction	Confidentiality
SAS-SAS data exchange	+	+	+	+	Hybrid
SAS marketplace	+	+	+	+	Hybrid
Sensing as a service	+	+	+	+	Hybrid
Element tracking	+	+	+	+	Hybrid
Neutral hosting	+	+	+	+	Hybrid
Operator roaming	+	+	+	+	Hybrid
CBSD measurements	+	−	±	−	Private
FCC database	−	−	−	−	Private
ESC sensing	+	+	−	−	Private

5 Conclusion

In this paper, we have developed and analyzed blockchain use cases for the novel spectrum sharing concept. This study discussed the implementation considerations of the CBRS spectrum sharing concept, and how the BC technology can be applied as a potential solution. We argue that the BC technology has potential to significantly reduce transaction costs in the CBRS through automatization of business-to-business complex multi-step workflows in contracting, brokering and data exchange. It codifies and controls negotiation principles required in contracting like consensus, provenance, immutability and finality. Furthermore, flexibility and scalability introduced into regulation and spectrum management lower the entry barrier and enable new entrants to access local spectrum based on their specific business needs. The BC contribute to transition from administrative to market-based spectrum management. Results of our analysis show that the automatization with cryptographic verifiability increase and build trust between key stakeholders and devices, which is essential trigger for any sharing concept. We believe that the integration of BCs in the spectrum management and control processes have potential to transform traditional MBB ecosystem, bring in new players and impact future system designs. Increased system dynamics in spectrum sharing will introduce a need for near real time network management capabilities that could benefit of IoT type P2P BC transactions of data, assets or services. Technology harmonization and integration with legacy in ecosystems will be essential to ensure economies of scale and fast time to market. Hybrid and private BC options will help in meeting the confidentiality requirements.

This paper serves as a starting point for analyzing the applicability of the BC technology and its key characteristics around the CBRS. Future work is needed to dwell deeper into studying and validating the core characteristics of the BC for the key stakeholders and their particular use case requirements in the CBRS context. Potential deployment considerations in the CBRS context calls for focused research in the areas of legal enforceability, transactional confidentiality, and consensus mechanism determination. The successful deployment of the BC technologies has potential to significantly improve the efficiency of the dynamic spectrum sharing concepts, influence the regulatory and management approaches of spectrum and create new business opportunities. This calls for a collaborative effort from the government, industry and academia to build and validate dynamic capabilities and technology enablers needed.

Acknowledgments. This work has been done in the microOperator (μO) and the Micro-operator concept for boosting local service delivery in 5G (uO5G) research projects within the 5G programs of Tekes - the Finnish Funding Agency for Technology and Innovation. The author would like to acknowledge the project consortium members: Aalto University, University of Oulu, Elisa, Eltel Networks, Fairspectrum, University Properties of Finland, Verkotan, Finnish Ministry of Transport and Communications, Finnish Communications Regulatory Authority and Tekes.

References

1. ITU-R: Final Acts WRC-15. World Radiocommunication Conference, Radio Communication Sector of the International Telecommunication Union, Geneva (2015)
2. The White House: Realizing the Full Potential of Government-Held Spectrum to Spur Economic Growth. President's Council of Advisors on Science and Technology (PCAST) Report (2012)
3. Tapscott, D., Tapscott, A.: Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business and the World. Portfolio Penguin, London (2016)
4. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System (2008)
5. Kelly, J., Williams, A.: Forty Big Banks Test Blockchain-Based Bond Trading System (2016). http://www.nytimes.com/reuters/2016/03/02/business/02reuters-bankingblockchain-bonds.html
6. Oparah, D.: 3 Ways that the Blockchain will Change the Real Estate Market (2016). http://techcrunch.com/2016/02/06/3-ways-that-blockchain-will-change-the-real-estate-market/
7. Kar, I.: Estonian Citizens will soon have the World's most Hack-Proof Health-Care Records (2016). http://qz.com/628889/this-eastern-european-country-ismoving-its-health-recordsto-the-blockchain/
8. Lacey, S.: The Energy Blockchain: How Bitcoin Could be a Catalyst for the Distributed Grid (2016). http://www.greentechmedia.com/articles/read/the-energy-blockchain-could-bitcoin-be-a-catalyst-forthe-distributed-grid
9. Walport, M.: Distributed ledger technology: beyond block chain. U.K. Government Office for Science, London, U.K., Technical report (2016)
10. Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the internet of things. IEEE Access **4**, 2292–2303 (2016)
11. Mitola, J., Maguire, G.: Cognitive radio: making software radios more personal. IEEE Pers. Commun. **6**(4), 13–18 (1999)
12. Cabric, D., Mishra, S., Brodersen, R.: Implementation issues in spectrum sensing for cognitive radios. In: Proceedings of the 38th Asilomar Conference on Signals, Systems and Computers. Pacific Grove, pp. 772–776 (2004)
13. FCC: 03-287 the Commission's Rules to Permit Unlicensed National Information Infrastructure Devices in the 5 GHz Band. Federal Communications Commission (2004)
14. FCC: White Spaces. http://www.fcc.gov/topic/white-space

15. Ofcom: TV White Spaces Pilot. http://stakeholders.ofcom.org.uk/spectrum/tv-white-spaces/white-spaces-pilot/
16. ECC: Licensed Shared Access (LSA). ECC report 205 (2014)
17. FCC: Report and Order and Second FNPRM to Advance Availability of 3550–3700 MHz Band for Wireless Broadband (2015)
18. Chapin, J., Lehr, W.: Cognitive radios for dynamic spectrum access - the path to market success for dynamic spectrum access technology. IEEE Commun. Mag. **45**(5), 96–103 (2007)
19. Yrjölä, S., Matinmikko, M., Ahokangas, P.: Evaluation of recent spectrum sharing concepts from business model scalability point of view. In: IEEE International Symposium on Dynamic Spectrum Access Networks (DYSPAN), pp. 241–250 (2015)
20. Sohul, M., Yao, M., Yang, T., Reed, J.: Spectrum access system for the citizen broadband radio service. IEEE Commun. Mag. **53**(7), 18–25 (2015)
21. Patil, V.M., Patil, S.R.: A survey on spectrum sensing algorithms for cognitive radio. In: Proceedings of the 2016 International Conference on Advances in Human Machine Interaction, pp. 1–5 (2016)
22. WINNF Spectrum Sharing Committee. http://www.wirelessinnovation.org/spectrum-sharing-committee
23. FCC: 16-55: The Second Report and Order and Order on Reconsideration Finalizing Rules for Innovative Citizens Broadband Radio Service in the 3.5 GHz Band (3550–3700 MHz) (2016). https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-55A1.pdf
24. OFR: Electronic Code of Federal Regulations, Title 47: Telecommunication, Part 96 - Citizens Broadband Radio Service. The Office of the Federal Register (OFR) and the Government Publishing Office. http://www.ecfr.gov/cgi-bin/text-idx?node=pt47.5.96&rgn=div5
25. NTIA: Using On-Shore Detected Radar Signal Power for Interference Protection of Off-Shore Radar Receivers. Technical report 16-521. The US Department of Commerce, National Telecommunications and Information Administration (2016)
26. WInnF: SAS Functional Architecture. Spectrum Sharing Committee of the Wireless Innovation Forum (2016). http://groups.winnforum.org/d/do/8512
27. WInnF: WINNF-15-S-0112-V1.0.0 CBRS Operational and Functional Requirements. Spectrum Sharing Committee (SSC) of the Wireless Innovation Forum (2016)
28. FCC: sharing recommendations. Federal Communications Commission Technical Advisory Council Advanced Sharing and Enabling Wireless Technologies (EWT) WG (2016). https://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting92314/TACMeetingSummary9-23-14.pdf
29. Antonopoulos, A.M.: Mastering Bitcoin: Unlocking Digital Cryptocurrencies, 1st edn. O'Reilly Media, Inc, Sebastopol (2014)
30. Dicks, D., Sherrington, S.: Blockchains & its Impact on the Telecom Industry, Heavy Reading Reports (2016)
31. Tsai, W., Blower, R., Zhu, Y., Yu, L.: A system view of financial blockchains. In: IEEE Symposium on Service-Oriented System Engineering (SOSE), pp. 450–457 (2016)
32. Szabo, N.: Smart contracts: building blocks for digital markets. Extropy, no. 16 (1996)
33. Hyperledger Project, Linux Foundation (2016). https://www.hyperledger.org/
34. Ethereum, White Paper (2016). https://github.com/ethereum/wiki/wiki/White-Paper
35. Lauslahti, K., Mattila, J., Seppälä, T.: Smart Contracts – How will Blockchain Technology Affect Contractual Practices? ETLA Report no. 57 (2016). https://www.etla.fi/julkaisut/alykas-sopimus-miten-blockchainmuuttaa-sopimuskaytantoja/
36. Greenspan, G.: Four genuine blockchain use cases (2016). https://www.linkedin.com/pulse/four-genuine-blockchain-use-casesgideon-greenspan