Identity Management using Blockchain for Cognitive Cellular Networks

Saravanan Raju, Sai Boddepalli, Suraj Gampa, Qiben Yan, Jitender S. Deogun
Department of Computer Science and Engineering, University of Nebraska, Lincoln, Nebraska, USA

***Abstract*—Cloud-centric cognitive cellular networks utilize dynamic spectrum access and opportunistic network access technologies as a means to mitigate spectrum crunch and network demand. However, furnishing a carrier with personally identifiable information for user setup increases the risk of profiling in cognitive cellular networks, wherein users seek secondary access at various times with multiple carriers. Moreover, network access provisioning – *assertion*, *authentication*, *authorization*, and *accounting* – implemented in conventional cellular networks is inadequate in the cognitive space, as it is neither spontaneous nor scalable. In this paper, we propose a privacy-enhancing user identity management system using blockchain technology which places due importance on both anonymity and attribution, and supports end-to-end management from user assertion to usage billing. The setup enables network access using pseudonymous identities, hindering the reconstruction of a subscriber's identity. Our test results indicate that this approach diminishes access provisioning duration by up to 4x, decreases network signaling traffic by almost 40%, and enables near real-time user billing that may lead to approximately 3x reduction in payments settlement time.**

***Index Terms*—identity management, blockchain, assertion, authentication, authorization, accounting, privacy, performance**

I. Introduction

The number of cellular connections and human population are strikingly close, each estimated at around 7.5 billion. While machines currently account for only 300 million, this number is forecast to triple, surpassing a billion by 2020. Around this same time, it is estimated that there will be an aggregate of 8.9 billion cellular connections worldwide, achieving a penetration rate of 1.14 per capita [1].

As cellular services used by humans and between machines continue to grow, so does the volume of data and network traffic. Today, the total monthly cellular data traffic is pegged at 8 exabyte, slated to be eight times this figure at the start of the next decade. In the case of smartphones, social networking ranks as the second largest traffic generator behind video streaming [2].

With cellular services becoming the primary means for people to interact socially and stay connected, ubiquitous systematic observation of all subjects rather than a select few has become the new normal. The growth in cellular connections and data traffic exposes avenues for profiling and increases privacy threats, now more than ever. These threats to an individual's right to privacy originate from institutions that include pernicious elements, private enterprises, and public entities [3]. As a result, issues regarding data collection and individual privacy have entered public discourse.

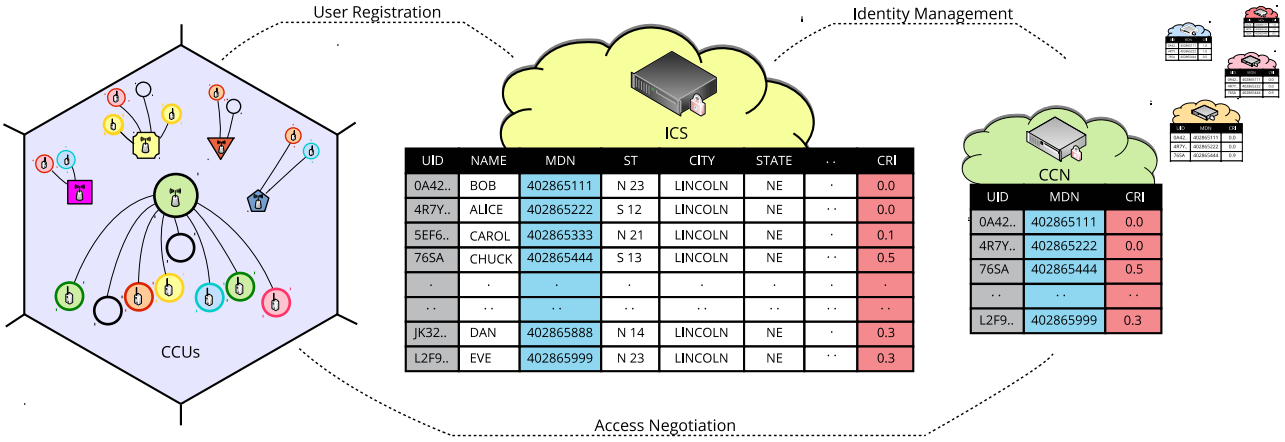
In [4], we proposed a cloud-centric cognitive cellular network (CCN) model to actualize dynamic spectrum access, facilitating carrier-agnostic, spontaneous provisioning of unaccredited users that spans the entire lifecycle, from assertion to accounting. We introduced *Identity and Credibility Service* (ICS) as a federated network element to ascertain the legitimacy of a cognitive cellular user (CCU). The ICS partners with CCNs and CCUs to provide user – subscriber and device – assertion, authentication, and authorization services. However, this setup neither accounted for nor was it equipped with mechanisms to execute service contracts, enable payments settlement, and more importantly, enhance user privacy. We address these insufficiencies in our work by using *blockchain* [5] technology to build the ICS.

A blockchain is a ledger to store cryptographically secured records. A blockchain network has multiple users, where each user is designated a pseudonymous identity. A contract dictates the interactions between the users and the ledger. The use of pseudonymous identities in a blockchain network presents the possibility of separating the identity provider from the network operator, with cryptographic contracts governing user data access. Hence, it is vital to study blockchain for identity management in the cellular domain to enhance privacy.

In this paper, we design the ICS using the privacy-enhancing blockchain protocol (BCP) with the CCNs and CCUs as participating nodes, and test BCP's performance against current network access protocols. We submit, to the best of our knowledge, we are not aware of any existing work on user identity management in cellular networks using blockchain. Our approach presents these benefits:

1) uses shared secrets to prevent unauthorized access to a subscriber's personally identifiable information necessary for user assertion,
2) limits data exposure by partitioning the blockchain data store so that only the pseudonymous identity of a subscriber is required for access provisioning,
3) enables app-specific credentials distinct from a user's network access credentials, which hinders the reconstruction of a subscriber's identity, and
4) supports a self-contained system with the necessary structures to accommodate user setup, access contracts, and usage billing.

The remainder of the paper is organized as follows: Section II discusses related work, Section III network setup, and Section IV experimental analysis. Section V presents final remarks.



UID	NAME	MDN	ST	CITY	STATE	..	CRI
0A42..	BOB	402865111	N 23	LINCOLN	NE	.	0.0
4R7Y..	ALICE	402865222	S 12	LINCOLN	NE	..	0.0
5EF6..	CAROL	402865333	N 21	LINCOLN	NE	.	0.1
76SA	CHUCK	402865444	S 13	LINCOLN	NE	..	0.5
.	.	.	.	.	.	.	.
..	..	..	..	..	..	..	..
JK32..	DAN	402865888	N 14	LINCOLN	NE	.	0.3
L2F9..	EVE	402865999	N 23	LINCOLN	NE	..	0.3

UID	MDN	CRI
0A42..	402865111	0.0
4R7Y..	402865222	0.0
76SA	402865444	0.5
..	..	..
L2F9..	402865999	0.3

Fig. 1. Reference Network Setup of a Private ICS Blockchain: The ICS assigns a pseudonymous UID to a CCU after user assertion. During secondary access, a CCU has to provide only its MDN and UID to a CCN. Use of UIDs increases privacy and hinders profiling.

II. Related Work

The protocol used across the telecommunications industry to administer AAA is Diameter [6]. It is the lingua franca for signaling between network elements, accounting for 70% of all signaling traffic. By 2020, this protocol is expected to surpass all global IP traffic by generating an estimated 395 million messages per second [7].

The growth in signaling traffic can be directly attributed to an increase in teledensity, particularly cellular communications. As teledensity increases, it presents two sets of challenges: one from an *ethical* viewpoint with regard to subscriber profiling and individual privacy, and the other from an *engineering* standpoint that concerns radio spectrum and network demand.

Ethically, the "walled garden" approach to network access and data services results in unprecedented user profiling by governments and businesses alike [3], [8]. The adoption of blockchain [9] can aid in the realization of trusted computing [10]. In the context of engineering, as radio spectrum demand grows, implementation of cognitive radio networks becomes imperative [11]. These networks enable dynamic spectrum access, but as users seek secondary network access from multiple carriers, more personal data has to be shared with multiple parties.

We therefore reason that in the realm of cognitive cellular networks, established AAA protocols have limitations in enhancing subscriber privacy and guaranteeing spontaneous network access. We assert that a network built using BCP can provide a comprehensive framework to address these shortcomings. Our design takes a contracts-based approach to dynamic spectrum and opportunistic network access. It addresses some of the real-world challenges outlined in [12] related to usage billing and payments settlement, while also having provisions to facilitate service contracts in a privacy-enhancing fashion [9], [13]. Notably, the pseudonymous nature of BCP assures both anonymity and attribution by separating a user's personal data from access data.

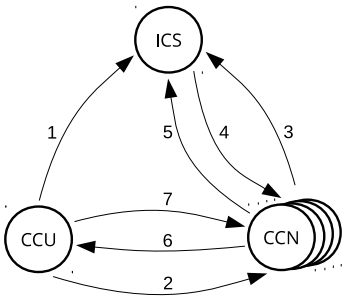
III. Network Setup

The topology is set up as a cloud-centric cognitive cellular network, as presented in [4] utilizing virtualized network elements, which adds elasticity to spectrum and network management.

The architecture is a two-layered federated access model, as shown in Fig. 1, where a CCN is both the spectrum owner and the network operator. A CCN operates in two modes: *primary network* (PN) and *secondary network* (SN), and services two distinct classes of CCUs: *primary user* (PU) and *secondary user* (SU) [11]. A PU receives service primarily from a PN, but it may also seek service as an SU from one or more SNs depending on the payoff offered. The SUs are unaccredited users of whom the SNs have no knowledge. The Network Access Exchange (NAE) supplies the CCUs with access contract options and the CCNs work with the ICS to handle user identity assertion and contract management. In addition, the CCNs poll the ICS to determine the number of CCUs in a given geolocation which will aid the CCNs in capacity planning and competing for new customers.

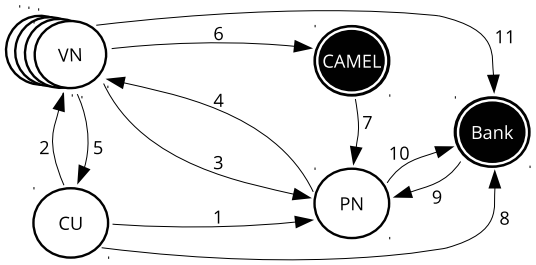
A. Blockchain

A blockchain is a secure, distributed database that in its most elementary form is a digital ledger. This ledger leverages peer-to-peer technology to list and link continuously added records, where each record is termed a *block*. All blocks are cryptographically signed and secured from accidental changes or adversarial tampering. Each new block stores a set of transactions and registers the hash of its preceding block to form a *chain* of blocks. A blockchain network has a number of users and every user has an assigned pseudonymous ID, for instance, `0x720c5d4eec51894b848e0bb362b3bbdfd655b375`. There are three network permissioning classes: *public*, *consortium*, and *private*. The ICS is a private chain that grants users network access only after assertion and approval [9]. The interactions between the ICS, CCNs, and CCUs are governed by *smart contracts* as elaborated in Section III-D.



1. User registration
2. Access request (NAR)
3. Known user
4. Validate identity(KYC)
5. Approve contract(KSC)
6. Access granted
7. Pay bill

(a) BCP signaling: Network access management from user assertion to bill payment is within the CCN ecosystem.



1. User registration
2. Access request
3. Identity request
4. Validate identity
5. Access granted
6. Usage statement
7. Forward statement
8. Pay bill
9. Credit money
10. Pay interconnect
11. Credit money

(b) AAA signaling: Entities enabling seamless secondary access and bill payment are outside the carrier's ecosystem.

Fig. 2. Comparison of Network Access Signaling Flow: BCP vs. AAA

B. User Provisioning

There are two objectives to user provisioning, one to assert the identity of a subscriber and the other to verify the compliance of a device with regulatory requirements. During the assertion process, a CCU supplies the ICS personally identifiable information (PII), such as first name, last name, address, etc. The ICS obtains the mobile directory number (MDN) a PN has assigned the CCU, and subsequently generates a pseudonymous blockchain ID (UID) to uniquely identify the subscriber's account. The MDN is the subscriber's phone number, and the UID is an alphanumeric string similar to the one mentioned in Section III-A.

All account information pertinent to a CCU (D_{CCU}) is partitioned into two sets, one to facilitate attribution (D_{PII}) in order to maintain legal compliance, and another (D_{NAX}) to enable service provisioning, as given in (1):

$$D_{CCU} = D_{PII} \cup D_{NAX} \tag{1}$$

$$D_{PII} \cap D_{NAX} = \{UID, MDN\} \tag{2}$$

To facilitate network access, the ICS shares with a CCN the data from (2) and a CCU's credit risk indicator (CRI) to let a CCN decide the level of network authorization the CCU should have. The risk index, CRI, may be derived from multiple parameters such as a subscriber's credit history, past usage etiquette, etc., where a high score implies a high risk. In this setup, a CCN may still collect metadata such as physical location, call records, websites visited, usage pattern, etc. for a given MDN, but cannot associate it directly with a real person. Likewise, the ICS only has data that the CCU supplied during identity assertion. This separation of personal and metadata enhances personal privacy and impedes subscriber profiling. Furthermore, the system is scalable, as CCNs need not have an interconnect agreement with each other. As a result, the architecture can grant opportunistic network access by spontaneous provisioning of SUs [4].

C. Service Provisioning

In conventional cellular networks, when a user requires network access while away from the home network, the request may be brokered by an application such as Customized Applications for Mobile networks Enhanced Logic (CAMEL) [14]. CAMEL is a suite of interconnect protocols to enable voice and data for subscribers in a visited network (VN). Periodically, carriers exchange usage information and settle any interconnect charges through banks using traditional financial tools, such as the Automated Clearing House (ACH) [15].

After a CCU enters into an access agreement with a CCN, the latter assigns a Mobile Identification Number (MIN) to the CCU's device. The MIN acts as a pointer to the subscriber's MDN i.e. $MDN \leftarrow MIN$. When a CCU switches between CCNs, each CCN activates a MIN pointing to the MDN. This interconnect setup based on number portability ensures a CCU receives voice calls bound to its MDN, irrespective of the CCN of which it is a customer.

D. Smart Contracts

The interactions between a CCU and a CCN are governed by a *smart contract* [9] facilitated by the ICS for the transactions shown in Fig. 2a. A smart contract in a blockchain network is a complete set of instructions programmed to run when prescribed conditions are met. A contract comprising of data and logic resides in the blockchain network once signed into motion and until such time it is ready to execute. Smart contracts have two broad purposes. First, they enforce privacy compliance between the CCU and the ICS with the intent of deterring unapproved access to personal data, and second, to establish a service level agreement between a CCU and a CCN for network access. Once a CCU and a CCN enter into a smart contract, it is then maintained and executed by the ICS blockchain network. The contract clauses may include provisions for arbitration, termination, choice of law, etc. that protects the interests of customers and carriers alike.

E. Security

A blockchain network such as ICS relies on public-key cryptography for transaction management. A CCU's account data is comprised of the 3-tuple cryptosystem, K_{CCU}:

$$K_{CCU} = (KR_{CCU}, KU_{CCU}, UID_{CCU}) \tag{3}$$

The ICS assigns a CCU a unique pseudonymous address, UID_{CCU}, derived from the hash of the CCU's public key, KU_{CCU}. A CCU relays its UID to the CCNs when requesting secondary network access. We assume no one but the CCU has access to its private key, KR_{CCU}.

Apart from CCUs, the ICS as well as each of the CCNs have their own UIDs with which contract policies and payment settlements between the CCUs and CCNs are handled. The ICS provides the following privacy enhancements for a user, and security benefits to a carrier:

1) User-centric: While the CCN does not know of a CCU's PII, the ICS has access to this data. Hence, after successful completion of the identity assertion process, the CCU's PII provided to the ICS is encrypted. The secret key used for encrypting the PII – $KS_{CCU,ICS}$ – is split and shared between the CCU and the ICS using Shamir's secret sharing scheme. This transaction's outcome is hashed and sent to the blockchain for entry. The rules that govern access to a subscriber's data are defined in the contract, $SC_{CCU,ICS}$. Thus, any access or alteration to the PII cannot happen without the consent of the CCU.

The aforementioned approach to identity management adds a layer of deterrence to subscriber profiling. Nevertheless, having one unique identification number still allows many data services to reconstruct the identity of a subscriber based on high-resolution data and deep-learning techniques [3]. To prevent such reconstruction, apart from the UID, ICS allows a CCU to randomly generate multiple pseudonymous identities per account based on the KR_{CCU} and KU_{CCU} pair:

$$UID_{CCU} = \{x \in [1..n]\} \tag{4}$$

A CCU thereby has the option to provide app-specific identities instead of its UID or MDN to programs that track metadata related to a user such as places visited, call history, etc., as part of a transaction [10], [13].

2) Carrier-centric: Cognitive radio networks take the commons approach and rely on their users to gauge spectrum utilization level [11]. The realization of cloud-centric CCNs depends on CCU etiquette in honest spectrum sensing, reporting, and sharing. However, it is likely that a malicious CCU may either over- or under-report spectrum utilization.

To mitigate this issue, we rely on the blockchain's *consensus* mechanism [16]. The purpose of consensus is to ensure peer users in the network agree on a state before it is published in the blockchain [9]. If some CCUs were to intentionally or even inadvertently provide incorrect spectrum utilization data not inline with the consensus, a CCN will reject the record.

IV. Experimental Analysis

We use the Ethereum [17] blockchain implementation to emulate the ICS. Our experiments are carried out on *testnet* – a private, sandboxed Ethereum network. For the conventional cellular setup, the 389 directory server is used for AAA. Both networks are served on identical x86-64 dual processor machines clocked at 3.8 GHz, and stocked with 16 GB of RAM. The tests are run on CentOS GNU/Linux 7 platform. We use three machines, each a hop from the other, to mimic a user, network carrier and the federated identity manager. To compare how the BCP scales vis-a-vis the AAA, identical simulations are run on them. We use a simple key-based authentication method to simulate access requests. Access provisioning and signaling performance are analyzed for 2,500 users, blockchain partitioning based user provisioning for 10,000 users. Additionally, bill payments settlement time in BCP is also evaluated.

Algorithm 1 Network Access Provisioning

function NAR($UID_{CCU}, MDN_{CCU}, NAE_{AID}$) ▷ Net. Req.
  status ← *false*
  if ({UID_{CCU}, MDN_{CCU}} = *known*) **then**
    if ($CRI_{CCU} < CRI_{threshold}$) **then** ▷ CRI ∈ [0..1]
      status ← $KSC(UID_{CCU}, UID_{CCN}, NAE_{AID})$
      return *status*
    else
      return *status*
  else
    status, CRI_{CCU} ← KYC(UID_{CCU}, MDN_{CCU})
    repeat 4 to 8

function KYC(UID_{CCU}, MDN_{CCU}) ▷ Validate User Identity
  status ← *false*
  CRI_{CCU} ← 1 ▷ CRI = 1 implies highest risk
  if ({UID_{CCU}, MDN_{CCU}} = *known*) **then**
    $CRI_{CCU} \leftarrow CRI(UID_{CCU}, MDN_{CCU})$
    status ← *true*
    return {status, CRI_{CCU}}
  else
    return {status, CRI_{CCU}}

A CCU queries the NAE to identify a contract, NAE_{AID}, which provides the best service at the lowest cost. It initiates the contract by establishing contact with the corresponding CCN. The CCU relays its UID_{CCU} and MDN_{CCU} as part of this process. If it is an unknown SU, the CCN forwards the request to the ICS with the information supplied by the CCU. Finally, the ICS attempts to validate the CCU based on this information.

If user identity assertion is successful, as shown in the Function KYC in Algorithm 1, the ICS reverts to the CCN with a positive reply. The CCN in response instructs the ICS to execute the access service contract presented in the Function KSC in Algorithm 2 per the SU's request, granting the SU network access. On the other hand, if the user was recently authenticated and the network session duration is below the timeout limit, the CCN may instruct the ICS to execute the contract right away. A CCN relies on the CCU's risk index, CRI, provided by the ICS, to make a determination about whether to permit a user into its network, and establish appropriate service usage limits.

After the ICS receives instruction from a CCN to proceed with a CCU's access request, the contract is executed by the ICS on behalf of the two parties. The contract has provisions to manage various aspects of the transaction, which include service tier, access price, usage time, etc. as outlined in functions CHECKKSC and CREDITKSC in Algorithm 2. Once a contract goes live, it stays a resident program within the ICS until its fulfillment.

Algorithm 2 Access Service Contract

function KSC($UID_{CCU}, UID_{CCN}, NAE_{AID}$)
  sender $\leftarrow UID_{CCU}$
  receiver $\leftarrow UID_{CCN}$
  amount $\leftarrow$ price $\times$ useTime

  function CHECKKSC(TIME, TIER, NAE_{AID})
    if (useTime < TIME && useTier $\geq$ TIER) **then**
      return true
    else
      return false

  function CREDITKSC($UID_{CCU}, UID_{CCN}, NAE_{AID}$)
    if (enforceKSC(usageDuration, usageQoS, NAE_{AID})) **then**
      coinBalanceOf[*sender*]$-=$ *amount*
      coinBalanceOf[*receiver*]$+=$ *amount*
      coinTransfer(*sender, receiver, amount*)
      return true
    else
      return false

In Ethereum-based ICS, smart contract clauses for access provisioning and bill payment may be implemented as follows:

```
private contract 0x160722314270261..4625 {
   //Private contract between CCU and ICS
   addressCCU    0x226..62b3bbdfd655b375;
   addressICS    0x306..7a79ac5138f86792;
   struct customerdata  {
          address              idUID;
          string               idState;
          string               nameFirst;
          string               nameLast;
          string               address;
    }
   function    validateIdentity()
          event subscriberIDcheck;
          event subscriberCreditCheck;
          ..
          event deviceESNCheck;
}
```

The aforementioned representational code is for a private contract between a CCU and the ICS, and the following is a public contract between a CCU and CCN:

```
public contract 0x1603141010FON23..74f3 {
   //Public contract between CCU and CCN
   addressCCU    0x226..62b3bbdfd655b375;
   addressCCN    0x524..75ad2967a1278cef;
   function  accessRequest()
          address            AID;
                  ..
          int                SLI;
          int                NAP;
   function  creditMoney()
          coinBalanceOf[addressCCU] -= amount;
          coinBalanceOf[addressCCN] += amount;
          coinTransfer(addressCCU, addressCCN, amount);
}
```

We gauge how BCP's access provisioning and network signaling fare in comparison to AAA under identical conditions.

A. Access Provisioning Performance

The duration between an access request sent to a CCN and the request being granted is the authentication time. We use the average authentication time for a CCU under various loads as the benchmark to compare the access provisioning performance of BCP and AAA. Two batches of tests are carried out: one with negligible latency and the other with an average regional latency of 36 ms as published in [18]. We observe from Fig. 3 that BCP outperforms AAA by up to 4x. The average time per successful authentication, in the absence and presence of latency, is 0.54 s and 0.72 s for BCP, and 1.52 s and 1.69 s for AAA. The results show that BCP will outperform AAA, particularly for short-term contracts.

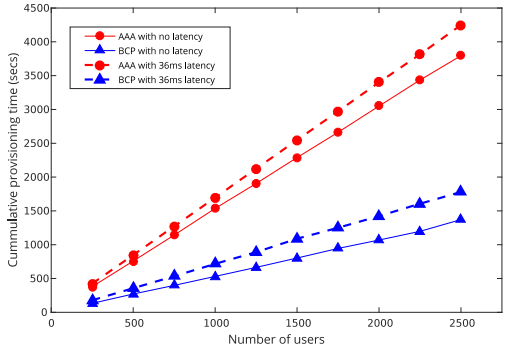


Fig. 3. Access Provisioning – BCP vs. AAA

B. Network Signaling Performance

Signaling is a vital component of network traffic that impacts a network's responsiveness. We conduct an elementary analysis of signaling performance in BCP and AAA by assigning a weight of one for each interaction a network element in Fig. 2 has with another in order to achieve user access provisioning. From Fig. 4 one may infer that the AAA trails behind BCP as the number of users increases.

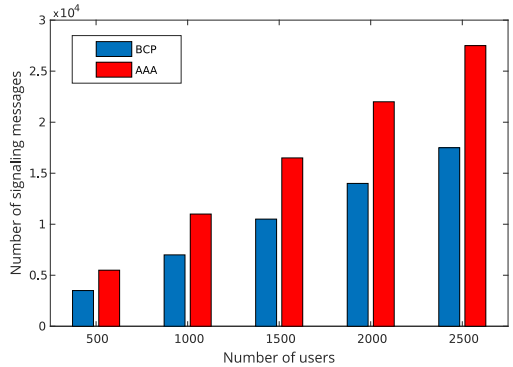


Fig. 4. Network Signaling – BCP vs. AAA

Unlike conventional cellular networks, the ICS that is built using BCP reduces signaling traffic by as much as 40%, as many of the network entities traditionally external to the setup, such as financial institutions to settle payments, are now within the ICS ecosystem.

C. Blockchain Partitioning Performance

As the number of blocks in a blockchain continues to grow, transaction throughput decreases [19]. The blockchain data store may be semantically partitioned to improve responsiveness.

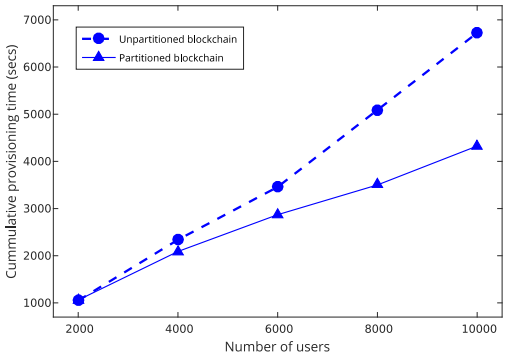


Fig. 5. BCP performance - Partitioned vs. Unpartitioned

We analyze network access provisioning performance by partitioning the ICS, which uses a simple key-value data store to group users based on postal codes in a given cell sector. As shown in Fig. 5., blockchain partitioning leads to faster access provisioning times as the number of subscribers and devices increases.

D. Payments Settlement Performance

With regard to usage billing, the current mechanisms to settle payments is time-consuming for CCNs who grant opportunistic network access to transitory secondary users. In the case of ACH, it takes two or three business days for payment realization [15]. ICS billing transactions use crypto-currencies as opposed to fiat currencies. Payments settlement in this design was processed on average in 500 milliseconds in our setup and may be realized in minutes [19] in the real world, yielding a conservative 3x reduction in settlement times. More importantly, the assurance of a smart contract adds a binding agreement on the CCUs to apportion funds for network usage, and the CCNs to allot network resources, at the time of access approval.

V. Final Remarks

We face engineering and ethical quandaries as cellular penetration and data consumption continue to grow. In order to safeguard personal privacy, a holistic approach to data security is a must. We propose a privacy enhancing identity management system using blockchain as a possible solution. The system strictly demarcates personal and access data, while still providing mechanisms for unaccredited users to obtain opportunistic network access in cognitive cellular networks. On evaluating the performance of our prototype against conventional methods, we note that the test results hold potential promise: a 4x improvement in access provisioning times, 40% decrease in signaling traffic, and 3x reduction in payments settlement time. In the future, we plan to test the model's scalability, and resistance against security attacks.

References

[1] Groupe Spécial Mobile Association, *2016 Mobile Industry Impact Report: Sustainable Development Goals*, ser. United Nations Private Sector Forum. Deloitte Touche Tohmatsu Limited on behalf of GSMA, Sept. 2016, Accessed on 2017-02-13. [Online]. Available: http://www.gsma.com/betterfuture/wp-content/uploads/2016/09/_UN_SDG_Report_FULL_R1_WEB_Singles_LOW.pdf

[2] Telefonaktiebolaget L. M. Ericsson, *Ericsson Mobility Report: On the Pulse of the Networked Society*, ser. Revision A. Anette Lundval, Sept. 2016, Accessed on 2017-02-13. [Online]. Available: https://www.ericsson.com/assets/local/mobility-report/documents/2016/ericsson-mobility-report-november-2016.pdf

[3] B. Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, 1st ed. W. W. Norton & Company, Mar. 2015, ISBN 978-0-393-35217-7.

[4] S. Raju, S. Boddepalli, Q. Yan, and J. S. Deogun, "Achieving 5As in Cloud Centric Cognitive Cellular Networks," in *2016 IEEE Global Communications Conference (GLOBECOM)*, Dec. 2016, pp. 1–6.

[5] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Oct. 2008, Accessed on 2017-02-13. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[6] M. Nakhjiri and M. Nakhjiri, *AAA and Network Security for Mobile Access Radius, Diameter, EAP, PKI and IP Mobility*, 1st ed. John Wiley & Sons, 2005, ISBN 978-0-470-01194-2.

[7] Oracle Communications, *Diameter Signaling Router*. Oracle Corporation, Oct. 2015, Accessed on 2016-07-22. [Online]. Available: http://www.oracle.com/us/industries/communications/diameter-signaling-router-ds-2100660.pdf

[8] J. Kleinsman and S. Buckley, "Facebook Study: A Little Bit Unethical But Worth It?" *Journal of Bioethical Inquiry*, vol. 12, no. 2, pp. 179–182, 2015, ISSN 1872-4353.

[9] M. Swan, *Blockchain: Blueprint for a New Economy*, 1st ed. 1005 GRAVENSTEIN HWY N., SEBASTOPOL, CA 95472, USA: O'Reilly Media, Feb. 2015, ISBN 978-0-393-35217-7.

[10] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in *Security and Privacy Workshops (SPW), 2015 IEEE*, May 2015, pp. 180–184.

[11] J. M. Peha, "Sharing Spectrum through Spectrum Policy Reform and Cognitive Radio," *Proceedings of the IEEE*, vol. 97, no. 4, pp. 708–719, Apr. 2009, ISSN 0018-9219.

[12] D. M. Kalathil and R. Jain, "Spectrum Sharing through Contracts for Cognitive Radios," *IEEE Transactions on Mobile Computing*, vol. 12, no. 10, pp. 1999–2011, Oct 2013, ISSN 1536-1233.

[13] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," in *2016 IEEE Symposium on Security and Privacy (SP)*, May 2016, pp. 839–858, ISSN 2375-1207.

[14] GSMA, "Mobile SMS and Data Roaming Explained," in *Groupe Spécial Mobile Association*, Mar. 2012, Accessed on 2017-02-13. [Online]. Available: http://www.gsma.com/aboutus/wp-content/uploads/2012/03/smsdataroamingexplained.pdf

[15] M. Ziolkowski, "Same Day Automated Clearing House," in *ABA Bank Compliance*. American Bankers Association, September 2016, vol. 37, pp. 16–19, ISSN 0887-0187.

[16] S. Raju, S. Boddepalli, N. Choudhury, Q. Yan, and J. S. Deogun, "Design and Analysis of Elastic Handoff in Cognitive Cellular Networks," in *Communications (ICC), 2017 IEEE International Conference on*, May 2017, pp. 1–6.

[17] G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," *Ethereum Project Yellow Paper*, July 2014, Accessed on 2017-02-13. [Online]. Available: http://gavwood.com/paper.pdf,http://www.ethereum.org

[18] SprintLink, "SLA Performance," in *Sprint Corporation*, Feb. 2017, Accessed on 2017-02-13. [Online]. Available: https://www.sprint.net/sla_performance.php

[19] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. Gün Sirer, D. Song, R. Wattenhofer, J. Clark, S. Meiklejohn, P. Y. Ryan, D. Wallach, M. Brenner, and K. Rohloff, "On Scaling Decentralized Blockchains: A Position Paper," in *Financial Cryptography and Data Security: FC 2016 International Workshops, BITCOIN, VOTING, and WAHC*. Springer, Aug. 2016, ch. 8, pp. 106–125, ISBN 978-3-662-53357-4.