Aplicação da Blockchain em problemas de Engenharia de Telecomunicações

Pedro L. de Oliveira, Murilo Dourado, Guilherme P. Aquino, Alessandra C. Domiciano, Francisco A.S. do Carmo
Instituto Nacional de Telecomunicações - Inatel
pedro.lopes@get.inatel.br, murilodourado@get.inatel.br, guilhermeaquino@inatel.br,
alessandracarolina@get.inatel.br, francisco.assis@inatel.br

***Resumo*—Uma *blockchain* é, nos mais simples termos, uma série de registros imutáveis de blocos de dados imutáveis que são gerenciados por grupos de computadores. Cada um destes blocos de dados é seguro e ligado a outros blocos de dados utilizando princípios criptográficos. Portanto, como principal característica, a *blockchain* ajuda a garantir a validade de uma transação registrando-a não apenas em um registro principal, mas também em um sistema distribuído conectado de registros, todos conectados por meio de um mecanismo seguro de validação.**

Originalmente, a *blockchain* foi criada para propósitos relacionados ao *bitcoin* [1], sendo a base tecnológica para as criptomoedas atuais. No entanto, essa tecnologia não está limitada a essa aplicação e, com isso em mente, foram pensados novos cenários para sua utilização, exclusivamente na área de Engenharia de Telecomunicações e que serão apresentados neste documento.

***Index Terms*—Blockchain, IoT, Validação de serviços, Registro Seguro da Gestão de Mudanças, Bilhetagem.**

I. Introdução

A *blockchain* nada mais é do que uma lista de registros e acontecimentos, disposta em formato de blocos. Esses blocos são criados em formato de corrente, em que cada bloco existente está ligado a um bloco sucessor e a outro bloco antecessor, dessa forma possibilitando que as informações desejadas fiquem salvas dentro dessa cadeia de blocos [2]. Além disso, ela se mostra revolucionária por conter três principais pilares que a sustentam. O primeiro pilar é a transparência, ou seja, todos os dados já escritos dentro de cada bloco podem ser acessados a qualquer momento e por qualquer usuário. Logo em seguida vem o quesito da imutabilidade, ou seja, tem-se se a vantagem de saber que todas as informações contidas nela jamais foram ou serão alteradas. Por fim está a característica de ser uma tecnologia que atua de forma descentralizada, assim se tornando praticamente impossível de ter seus dados fraudados, pois sua rede não estará em apenas um servidor, mas sim em todas as máquinas que fazem parte da cadeia de blocos.

A blockchain hoje é a base tecnológica para todas as criptomoedas existentes. No entanto, sua utilização ultrapassa o universo das criptomoedas e pode ser usada para os mais diversos fins como, contratos inteligentes, pagamento virtual, crowdfunding, armazenamento de arquivos, proteção de propriedade intelectual e, também, dentro da engenharia de telecomunicações [3].

Basicamente, a blockchain pode ajudar as operadoras de serviços de telecomunicações a se prevenirem de fraudes [4], que definham suas receitas financeiras, bem como, a gerirem melhor as identidades dos seus usuários [5], prevenindo que os mesmos sofram algum ataque de autenticação. Além disso, a blockchain pode ser uma boa solução ao problema de segurança que afligem os sistemas de Internet das coisas (IoT — *Internet of Things*) [6].

O objetivo deste trabalho de iniciação científica é apresentar um estudo preliminar sobre a utilização da blockchain em problemas relacionados à engenharia de telecomunicações. Nesse artigo foram explorados mais a fundo um total de 2 problemas que podem ser resolvidos com a *blockchain*, aqui denominados de: i) validação de serviços prestados por provedores de acesso à Internet, ii) falha de bilhetagem de usuários de telefonia. Outros dois problemas levantados durante o estudo também são apresentados nesse artigo, porém, de forma mais sucinta: iii) validação de comunicação M2M (Machine-to-Machine), iv) validação de mapas de cobertura e v) Registro seguro da gestão de mudanças. Esses três últimos sugerem uma continuação desse estudo aqui apresentado.

Para cumprir com o objetivo desse artigo, o mesmo se encontra organizado da seguinte forma. A Seção II traz uma abordagem fundamental sobre a *blockchain*. A Seção III traz uma análise sobre o problema de validação de serviços prestados por provedores de acesso à Internet (ISP – *Internet Service Provider*) e mostra um experimento criado durante esse estudo para demonstrar como a *blockchain* pode resolver esse problema. A Seção IV apresenta uma análise sobre o problema da falha de bilhetagem em sistemas de telefonia e mostra um experimento criado durante esse estudo para demonstrar como a *blockchain* pode resolver esse problema. A Seção V traz uma análise sucinta sobre outros problemas da área de engenharia de telecomunicações que podem ser resolvidos com o uso da *blockchain* e pode ser vista como uma seção de trabalhos futuros. Por fim, a Seção VI traz as principais conclusões obtidas com esse estudo.

II. Blockchain

Como já citado, a *blockchain* é formada por uma cadeia de blocos. Esses blocos possuem uma formatação que se adéqua à aplicação. Ou seja, para cada aplicação, o bloco é criado de uma forma distinta e com informações distintas dentro deles. Nesse trabalho, um bloco sempre será criado contendo a seguinte formatação:

Bloco[índice]:
Timestamp // Informação // Hash anterior // Nonce

A *timestamp* é basicamente uma formatação de data e hora, para que haja uma ordem cronológica das informações e da formação dos blocos. Também previne possíveis alterações, caso a obtenção dessa seja feita de forma automatizada. Geralmente uma *timestamp* tem o seguinte formato: DD/MM/YYYY hh:mm:ss.

O campo informação traz de fato o que será guardado no bloco. Portanto, se adequará a aplicação, podendo conter uma única informação específica, ou várias informações.

Antes de entender a necessidade do *hash* anterior na formatação do bloco é preciso entender o que é um *hash*, como ele é gerado e por fim, como ele é validado. O *hash* nada mais é que uma função de criptografia irreversível que ao receber em sua entrada uma determinada informação, que possui um tamanho qualquer, retorna um código de tamanho fixo em sua saída. Além disso, é importante que se saiba que dado o resultado de um *hash*, é impraticável, ou quase impossível, descobrir qual fora a informação tratada pela função. Ainda, as funções de *hash* geram saídas descorrelacionadas quando as entradas possuem diferenças discretas. Ou seja, uma minúscula alteração do dado de entrada, resultará em um valor completamente diferente na saída da função de *hash* [7]. Vale ressaltar que independente do tamanho da informação, o tamanho do *hash* é fixo. Existem inúmeras funções de *hash* na literatura. Nesse artigo a função de *hash* usada será a MD5.

A validação de um *hash* é feita através do conceito de nível de segurança (SL – *Security Level*). Que deve ser estipulado de acordo com a aplicação, que consiste, basicamente, no número de zeros no início do *hash*. Portanto, um *hash* com SL 5 é um *hash* com cinco zeros em seu início, como: 000007198086c86bda72b01d1e3bde19. O *hash* anterior nesse caso servirá como uma corrente, que atrela um bloco a outro, caso um bloco seja alterado, seu *hash* será alterado, e, consequentemente, seu sucessor também será alterado, uma vez que o *hash* do anterior é utilizado para formar o seu próprio.

Por fim, o *nonce* é o elemento que valida um conceito muito importante para a *blockchain*, a prova de trabalho (*Proof of Work*). Um *nonce* nada mais é que um número adicionado ao bloco, ou à informação do bloco, que altera seu *hash*. É com o *nonce*, que os *hashs* se tornam válidos. Para tal, a blockchain irá colocar valores aleatórios para o *nonce* e concatená-lo à informação. Ao gerar o *hash* dessa concatenação, verifica-se quantos zeros existem no início do mesmo. Para atingir o nível de segurança desejado é necessário encontrar um *nonce* que, adicionado à informação, forme um *hash* com zeros suficientes em seu início. Sendo assim, é necessário gastar processamento para que o *nonce* seja encontrado, ou seja, se ele foi encontrado, trabalho foi demandado. Por isso o nome do conceito é prova de trabalho.

Esse conceito de blocos será usado para solucionar os problemas de engenharia de telecomunicações apresentados no restante desse trabalho.

III. Validação de serviços prestados por ISPs

Um problema interessante do ponto de vista da engenharia de telecomunicações está relacionado ao fato de algum cliente conseguir verificar e provar se seu ISP está, de fato, oferecendo os serviços de acordo com os contratados.

A ideia proposta nesse estudo consiste em o usuário, ou uma operadora virtual, conseguir comprovar de maneira cabal (por meio da *blockchain*) que o serviço prestado pela operadora corresponde ao contratado pelo usuário em questão. A validação é feita com um relatório mensal, gerado através de uma aplicação feita na linguagem de programação *python*, que concatena informações de taxa de *download*, *upload*, conectividade da rede, data e hora de acesso em um bloco da *blockchain*. Esta aplicação é processada por um dispositivo ligado diretamente ao enlace de Internet que chega à residência do usuário. Esse, por sua vez, fará a obtenção do *nonce* e, consequentemente a formação do bloco. Aferindo os dados obtidos, com os assinados em contrato é possível que detectem incoerências e, quando estas ocorrerem, haverá a viabilidade de ser efetuado um ressarcimento pelos serviços não prestados.

Os dados estipulados para a validação dos serviços prestados pelo ISP são: Porcentagem de blocos mostrando que há conexão com a Internet, porcentagem de blocos mostrando que não há conexão, taxa média de transferência de dados de *download*, taxa média de transferência de dados de *upload* e *atraso*. A escolha foi feita baseada no montante de informações providas por uma das aplicações utilizadas, o `speedtest-cli`, que foi desenvolvido pelo serviço da SpeedTest.net.

A. Experimento e Resultados

Dada a proposta, atacou-se a situação problema que, novamente, é a existência de conflitos entre clientes contratantes de um serviço de Internet e seus respectivos provedores, quanto à qualidade dos trabalhos prestados. Para isso, foi construído um algoritmo que, baseado na ferramenta anteriormente citada (*Speedtest.net*) e aliado à *blockchain*, valida se o serviço prestado condiz com o contrato fechado.

O algoritmo construído é ilustrado por um diagrama de blocos mostrado na Figura 1.

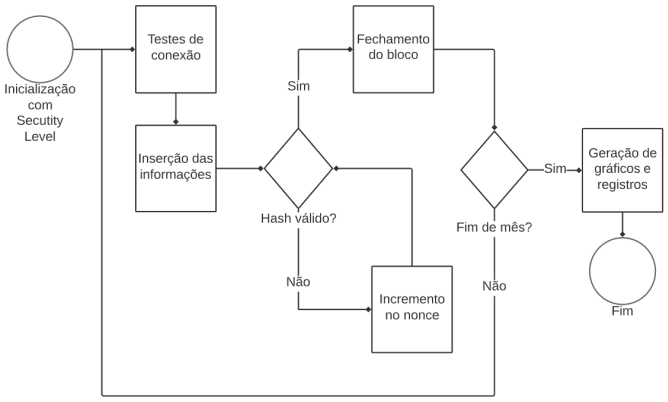

Figura 1. Diagrama em blocos do algoritmo de verificação de serviços prestados pelos ISPs.

O algoritmo criado permite que o usuário gere blocos de dados confiáveis contendo os dados de suas medições. Além disso, possibilita a criação de gráficos com médias diárias das

métricas. Além de também possuir um sistema de geração automática dos registros em arquivo cuja extensão é .txt, que por sua vez podem ser conferidos através de ferramentas computacionais. Finalmente, há uma ferramenta de busca que possibilita a pesquisa de blocos baseada em datas, tornando fácil encontrar os dados desejados em um dado momento específico.

Para fins de prova de conceito, foi realizado um experimento ao longo de uma semana com testes contínuos, ocorrendo em uma rede privada. Os resultados de tal experimento são exibidos nas Figuras 2, 3 e 4.

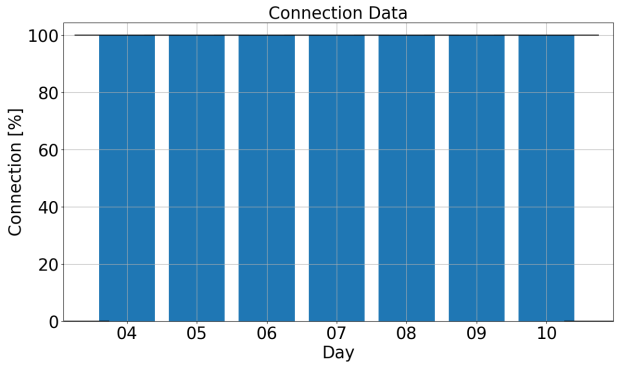

Figura 2. Porcentagem de sucesso ao realizar a tentativa de se conectar à internet

Pode-se perceber por meio da Figura 2 que durante os testes de conectividade com a Internet, o usuário obteve sucesso em todas as tentativas de conexão em todos os dias analisados.

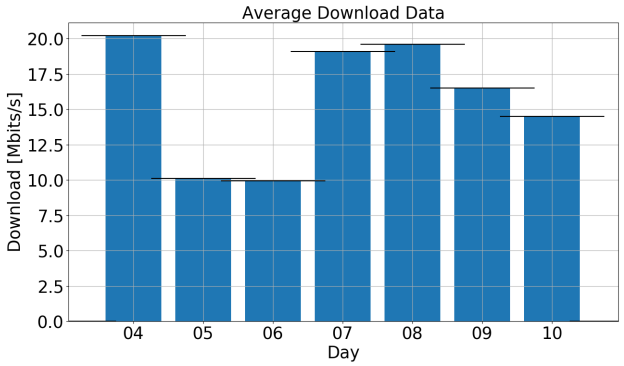

Figura 3. Taxa de *Downlink* experimentada pelo usuário, em Mbps

Por meio da Figura 3 é possível verificar qual foi a média da taxa de *download* experimentada pelo usuário durante todos os dias de testes. É possível verificar que a média da taxa de *download* varia entre 10 Mbps e 20 Mbps. Se o contrato do usuário estiver trazendo informações contrárias às experimentadas pelo usuário, esse terá como mostrar que o ISP não está cumprindo com o contrato. A mesma conclusões podem ser verificadas na Figura 4, porém, relacionadas à taxa de transferência de *upload*.

Além dos gráficos, a ferramenta criada também faz o fechamento de blocos, usando a mesma ideia da *blockchain*. Nesses blocos, todos os dados relacionados à conectividade e

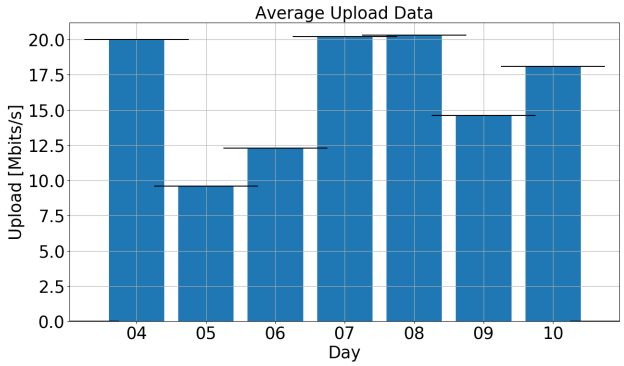

Figura 4. Taxa de *Uplink* experimentada pelo usuário, em Mbps

às taxas de transmissão e recepção de dados são registrados juntamente com o *hash* que mostram a prova de trabalho.

O Bloco formado após o processamento segue o seguinte padrão: Data e hora // Taxa de downlink // Taxa de uplink // Hash do bloco antecessor // Posição do atual bloco na cadeia // Nonce.

Sendo assim, um bloco real formado após o tratamento dos dados utilizados, é mostrado a seguir:

21/01/2020 21:56:14 // Status da rede: Conectado // Download: 3.61 Mbit/s // Upload: 2.32 Mbit/s // 000004188add8ffdd51c89838f293df1000c27114c36c412fc2f0c13cadaff0d // 1 // 298563.

Qualquer indivíduo que tenha acesso aos blocos poderão versificar a vericidade dos dados registrados no mesmo bloco. É importante mencionar que o teste feito corresponde apenas ao usuário fazer suas próprias medidas e registrá-las dentro dos blocos. Portanto, se trata apenas de uma prova de conceito. Para o perfeito funcionamento dessa ferramenta dentro de uma *blockchain*, será necessário que outros elementos na rede confirmem que as medidas feitas pelo usuário específico sejam verdadeiras.

IV. Falha de bilhetagem de usuários de telefonia

A falha de bilhetagem em rotas de interconexão é uma das falhas que mais prejudicam a receita da operadora de telefonia [8]. Tal falha ocorre quando, uma operadora de telefonia presta algum tipo de serviço para um cliente de outra, e esta não fica ciente de que seu usuário utilizou recursos da primeira. Com isso, a operadora que prestou o serviço cobrará a outra operadora, porém essa outra não arrecadará a quantia por parte do usuário, dessa forma arcando com os custos envolvidos.

Nesse estudo foi elaborada uma aplicação para se fazer a prova de conceito de como a *blockchain* pode resolver o problema de falha de bilhetagem. A aplicação consiste em suprir a *blockchain* com blocos cuja informação são CDR's (*Call Detail Records*) dos usuários. Um CDR é um registro produzido por uma conexão telefônica que pode conter a duração da chamada telefônica, os números envolvidos, falhas de conexão que foram encontradas, entre outros dados [9]. Portanto, com esses dados em mãos é possível que ao final de um ciclo de cobrança, o usuário seja cobrado pelo uso, uma

vez que será armazenado o tempo de utilização, localidade, recursos demandados e, consequentemente o valor envolvido para tal feito. Numa visão mais generalista, a *blockchain* irá prover o valor que cada operadora deve pagar para a outra e também quanto o usuário deverá pagar à sua própria operadora.

Contendo uma série de registros de CDRs na blockchain, as operadoras se certificarão que estão fazendo as cobranças de forma devida, eliminando o conflito de divergências entre elas. Quando uma dada operadora verificar, pelos registros confiáveis, que o seu processo de bilhetagem está falhando, ela poderá disparar ações que irão corrigir as falhas do processo.

A. Experimento e Resultados

A aplicação desenvolvida nesse estudo tem por base duas principais atividades: i) registrar de forma segura os CDRs gerados por centrais telefônicas dados e ii) calcular os valores que uma determinada operadora deve pagar para a outra operadora em uma rota de interconexão qualquer.

Para fazer um experimento mais realista, foram utilizados dois PABX (*Private Automatic Branch Exchange*) Ision IP 2000 da empresa Leucotron [10] interconectados por um tronco E1 que emula a rota de interconexão entre duas operadoras distintas. NA configuração feita, os telefones conectados aos PABXs podem se comunicar através de chamadas internas ou externas. Além do mais, tal equipamento tem a capacidade de aferir qual tipo de ligação foi realizada, onde esta ligação se originou e qual foi o seu destino, além de informar qual foi o tempo de utilização de cada ligação individualmente, montando assim o CDR desejado.

De posse dos dois PABXs, foram gerados inúmeros CDRs tanto para ligações internas quanto externas. Assim, a aplicação gerada nesse estudo deverá apenas coletar os CDRs que são gerados para as chamadas externas, que são de fato o objeto de estudo sobre a falha de bilhetagem. As chamadas internas foram realizadas para que o montante de CDRs em cada PABX fossem diferentes, tornando o cenário mais realista.

A aplicação desenvolvida utiliza linguagem *Python* e tem como objetivo tratar e criar blocos com as informações contidas nos CDRs coletados em cada um dos PABXs. A Figura 5 ilustra o diagrama em blocos da aplicação criada para análise das falhas de bilhetagem.

No início do processo, deve-se ler todos os CDRs gerados pelos PABXs. O CDR gerado pelo PABX Leucotron tem a seguinte formatação:

```
CDR Original: S4 400 01/11/19 15:51:52
15:51:52 00:31:41 00:31:41 00:00:04
00:00:00 t029 001 700.
```

Após o tratamento inicial feito pela aplicação criada, o CDR tratado irá possuir a seguinte mostrada a seguir. Perceba que foi inserida uma informação quanto ao custo da ligação, no caso 1901 ETH. Isso foi feito com base na duração da chamada, 1901 segundos e foi atribuido, apenas para prova de conceito, um valor a ser pago de 1 ETH [11] por segundo de duração da chamada. É importante mencionar que o ETH (Ethereum) é uma moeda virtual que será usada para se fazer um pagamento entre as operadoras. Essa moeda foi escolhida em função das facilidades que se tem para se usar a rede Ethereum para estabelecimento de contratos inteligentes [12].

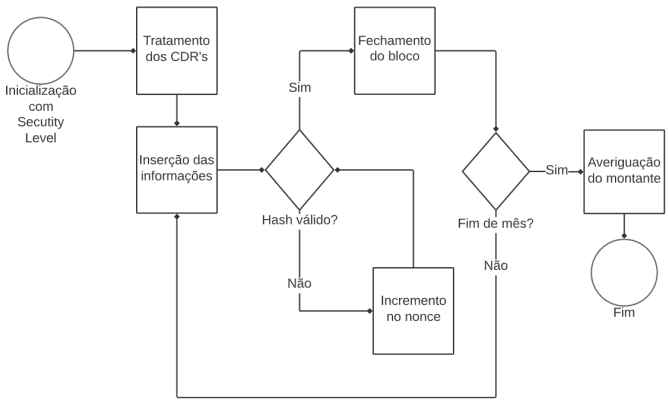

Figura 5. Diagrama de blocos do algoritmo Blockchain para averiguação de montante

```
CDR Tratado: Ligação: E / Origem: 400
/ Destino: 700 / Duração: 00:31:41 /
Efetuada em: 01/11/19 15:51:52 / Custo:
1901 [ETH].
```

Após o fechamento do bloco pela blockchain, tem-se o CDR validado cm a formatação mostrada a seguir. Perceba que o *hash* da prova de trabalho foi inserido no bloco, juntamente com as outras informações necessárias para a geração desse *hash*.

```
CDR em bloco: 06/11/2019 13:31:26
// 01/11/19 15:51:52 // 400 //
700 // 00:31:41 // Externa //
000009e7c9557ebe2a931ef4d11d36dae788391d
6dfe535c8312fc5fe38875bb // 2 // 3645500.
```

Dessa forma, os blocos podem ser acessados por qualquer operadora, e os resultados mostrados pelos CDRs validados podem ser analisados para fins de busca de possíveis sinais de falha de bilhetagem dentro dessa rota específica.

Ao final de cada mês a aplicação faz o cômputo do quanto uma operadora terá que pagar a outra. Ou seja, de posse de todos os CDRs validados, a aplicação calcula a diferença de tempo de chamadas entre as duas operadoras. Portanto, para que não haja conflito entre as partes, ambos os PABX, ao executarem o algoritmo proposto devem chegar à mesma conclusão, exemplificada abaixo através de uma mensagem na saída da aplicação:

```
"PABX1 deve pagar 527 [ETH] ao PABX2.",
```

que é gerada através de um bloco de tarifação, criado pela aplicação, que possui a seguinte forma:

```
05/11/2019 20:13:15 // Bloco de Tarifação
// PABX2 recebe // PABX1 paga //
527 [ETH] // Tarifação tipo 01 //
000005f995750c05d1fefee66d609 // 26 //
88562
```

Para fins de efetivar uma transação segura fora construído um *Smart Contract* provido pela rede *Ethereum*, utilizando-se da linguagem de programação *Solidity*, pois por meio deste é possível que ambas as partes tenham plena certeza, por meio de um algoritmo, que o montante só será distribuído se certas condições ocorrerem, nesse caso, quando ambos os PABX emitirem um relatório condizente.

V. Outros problemas de engenharia de telecomunicações que podem ser resolvidos com a *blockchain*

Além dos dois problemas apresentados anteriormente, durante esse estudo também foram levantados outros problemas que poderiam ser resolvidos com o uso da *blockchain*. Nessa seção, esses problemas serão colocados de forma sucinta e poderão ser melhores explorados em um estudo futuro.

O primeiro problema consiste em um registro seguro de gestão de mudanças. Basicamente, a ideia baseia-se em registrar na *blockchain* as atualizações feitas nos equipamentos de rede de uma dada empresa. Feito isso, é possível ter os registros de cada mudança já realizada, contendo o responsável pela mudança, quais foram as mudanças feitas, data e hora da mudança e também conter todos os demais dados que se façam necessários. Com isso, é possível obter-se um histórico confiável de todas as alterações na rede em questão, possibilitando que, caso haja algum problema ocasionado por uma modificação indevida no sistema, o responsável seja identificado prontamente. Além disso, uma base de *backups* confiáveis estará a disposição para se fazer um ponto de restauração. Nesse caso, os dados contidos no bloco seriam: Firmware anterior, firmware atualizado, autor/IP/máquina da alteração, data e hora.

Um segundo problema atende a uma área das telecomunicações com grande crescimento nos últimos anos, a Internet das coisas (IoT – *Internet of Things*). Essa área compreende todos os dispositivos que devem estar conectados a todo momento com a Internet e também aqueles que se comunicam entre si, gerando um tipo de comunicação entre máquinas, denominado de M2M (*Machine to Machine*). Muitas aplicações em IoT tem como principal fornecedor de informações os sensores, porém é necessário estabelecer uma conexão entre esses e o servidor dessas informações. Essa conexão muita das vezes não possui monitoramento ou segurança. Caso as informações sejam interceptadas e alteradas pode-se gerar uma falha em cadeia por se tratar de máquinas conversando. Um erro ou alteração pode acarretar em muitos outros. Com isso em mente, a *blockchain* é de extrema valia pelo seu quesito de descentralização, pois fazendo com que a informação chegue ao servidor por diferentes vias, a interceptação torna-se muito mais difícil, por fim, antes de gravá-la é necessário que cinquenta por cento dos nós mais um, concordem que a informação está correta. Vale ressaltar que de posse das localidades que enviaram informações incorretas, torna-se fácil a identificação e rastreamento de nós corrompidos.

O último problema em discussão se trata da validação de mapas de cobertura de operadoras. Em um estudo preliminar, pôde-se observar que os dados disponibilizados pelas operadoras em seus *websites*, não se mostram tão coerentes na prática. Normalmente as áreas de cobertura apresentados, mostram uma área de cobertura amplamente difundida. Porém, não parecem representar uma fidelidade com os dados observados na realidade, principalmente quando se leva em consideração zonas rurais e estradas. Sendo assim, é possível aplicar à *blockchain* os dados retirados da utilização dos próprios usuários da operadora, como potência do sinal recebido e latência, que dão uma boa margem para estimar se, naquele local, o serviço que virá a ser prestado será de péssima, má, boa ou ótima qualidade. Com um grande contingente de dados vindos dos celulares dos próprios usuários é possível estimar novos mapas de cobertura com maior confiabilidade e precisão, garantidos pela própria *blockchain*, o que possibilita ao futuro usuário escolher a melhor operadora para a localidade em que o mesmo se encontra.

VI. Conclusão

Visto o discorrer do trabalho, conceitos adquiridos e estudos realizados, concluiu-se que a tecnologia da *blockchain* se mostrou efetiva ao ser utilizada nos problemas de "Validação de serviços prestados por ISPs" e "Falha de bilhetagem de usuários de telefonia", uma vez que tais temas foram solucionados ao utilizar as provas de conceito, neste artigo, propostas. Além de que, fora constatado que os demais temas propostos são potencialmente solúveis ao se utilizar das ferramentas estudadas, e com a criação de cenários adequados.

Se faz válido ainda, incutir neste tópico o fato de haver espaço para um futuro estudo das soluções para as aplicações que não obtiveram suas provas de conceito edificadas

Referências

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," disponível em https://bitcoin.org/bitcoin.pdf.

[2] J. Lou, Q. Zhang, Z. Qi, and K. Lei, "A blockchain-based key management scheme for named data networking," in *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*, Aug 2018, pp. 141–146.

[3] A. Babu and B. Davis, "How blockchain can impact the telecommunications industry," Agosto 2016, disponível em https://www2.deloitte.com.

[4] S. Kou, H. Yang, H. Zheng, W. Bai, J. Zhang, and Y. Wu, "Blockchain mechanism based on enhancing consensus for trusted optical networks," in *Asia Communications and Photonics Conference*, Guangzhou, China, March 2017.

[5] Y. Sun, L. Zhang, G. Feng, B. Yang, B. Cao, and M. A. Imran, "Blockchain-enabled wireless internet of things: Performance analysis and optimal communication node deployment," *IEEE Internet of Things Journal*, 2017.

[6] F. Xu, F. Yang, C. Zhao, and C. Fang, "Edge computing and caching based blockchain iot network,," in *1st IEEE International Conference on Hot Information-Centric Networking*, Shenzhen, China, 2018.

[7] J. Fridrich and M. Goljan, "Robust hash functions for digital watermarking," in *Proceedings International Conference on Information Technology: Coding and Computing (Cat. No.PR00540)*, March 2000, pp. 178–183.

[8] C. E. S. Rosa and G. P. Aquino, "Uma simples metodologia para análise de perda de receita de operadoras telefônicas devido à falha de bilhetagem em rotas de interconexão,," in *Seminário De Redes e Sistemas de Telecomunicações do Instituto Nacional de Telecomunicações*, Santa Rita do Sapucaí, Brazil, 2014.
[9] O. Jukić and I. Heđi, "The use of call detail records and data mart dimensioning for telecommunication companies," in *2012 20th Telecommunications Forum (TELFOR)*, Nov 2012, pp. 292–295.
[10] Leucotron, "Ision IP, central telefônica PABX," disponível em: https://www.leucotron.com.br/pabx-ision-ip.
[11] Foxbit, "O que é ethereum?" 2017, disponível em: https://foxbit.com.br/o-que-e-ethereum/.
[12] A. Pinna, S. Ibba, G. Baralla, R. Tonelli, and M. Marchesi, "A massive analysis of ethereum smart contracts empirical study and code metrics," *IEEE Access*, vol. 7, pp. 78 194–78 213, 2019.