DOI 10.37882/2223–2966.2021.04–2.16

К ВНЕДРЕНИЕ ТЕХНОЛОГИЙ РАСПРЕДЕЛЕННЫХ РЕЕСТРОВ В ДОРОЖНУЮ ИНФРАСТРУКТУРУ V2X

IMPLEMENTING DISTRIBUTED LEDGER TECHNOLOGIES IN V2X ROAD INFRASTRUCTURE

A. Salagaev
S. Molodyakov

Summary. Blockchain technologies are defining a new decentralized paradigm for most traditional applications, where smart contracts provide a straightforward mechanism for decentralized governance. In this work, we propose an approach for decentralized V2X (D-V2X) that does not require any trusted authority and can be implemented on top of any communication protocol.

Keywords: intelligent transport systems, blockchain, security, privacy, identity, bluetooth low energy V2X, smart-contracts, directed acyclic graphs.

Салагаев Артем Андреевич
Аспирант, Санкт-Петербургский политехнический университет Петра Великого
gitsartem@gmail.com
Молодяков Сергей Александрович
Д.т.н., профессор, Санкт-Петербургский политехнический университет Петра Великого
molodyakov_sa@spbstu.ru
К Аннотация

Аннотация. Технологии блокчейн определяют новую парадигму децентрализации для большинства традиционных приложений, в которой смарт-контракты обеспечивают простой механизм децентрализованного управления. В этой работе предлагается подход для децентрализованного V2X (D-V2X), который не требует никаких доверенных полномочий и может быть реализован поверх любого протокола связи.

Ключевые слова: интеллектуальная транспортная система, блокчейн, безопасность, конфиденциальность, идентификация, Bluetooth с низким энергопотреблением, смарт-контракты, направленный ациклический граф, V2X.

Введение

В ближайшие несколько лет в автомобильном секторе промышленности произойдёт множество изменений, среди которых появятся новые услуги и предложения по обеспечению мобильности, что будет являться следствием глубоких технологических преобразований в этих секторах. Но одна вещь не изменится — водитель является единственным действующим лицом, ответственным за принятие решений в автомобиле.

Существует множество вариантов взаимодействия с «Подключённым автомобилем» (Connected Vehicle (CV)) [1]: V2V (между автомобилями); V2I (транспортная инфраструктура); I2V (от инфраструктуры до автомобиля); V2P (от транспортного средства к пешеходу); и V2X (от транспортного средства к чему-либо). Но, несмотря на современные технологии V2X, то есть C–V2X и 802.11p, необходимые для продвинутого автономного вождения, в течение ещё многих лет на дорогах будут водители-люди. Вождение — это децентрализованный процесс, где инфраструктура даёт некоторые рекомендации, но в конечном итоге водители взаимодействуют друг с другом, чтобы все работало. По мере того, как технологии V2X выходят на рынок, водители смогут пользоваться всей доступной дополнительной информацией, что приведёт к повышению безопасности дорожного движения и эффективности вождения.

Типичная связь V2X осуществляется в широковещательном режиме, когда некоторые элементы инфраструктуры или транспортные средства передают соответствующую информацию ближайшим транспортным средствам. В этих сценариях существуют различные требования безопасности, которые могут иметь значение [2]: аутентификация, целостность сообщения, контроль доступа, конфиденциальность сообщений, доступность, конфиденциальность и анонимность. Двумя основными факторами безопасности, которые должна обеспечивать любая интеллектуальная транспортная система (ИТС) являются аутентификация и целостность сообщений. Транспортные средства должны аутентифицировать отправителя полученных сообщений и быть уверенными, что их целостность сохраняется, прежде чем использовать какую-либо информацию в этих сообщениях. Конфиденциальность не так важна для коммуникаций ИТС, поскольку информация обычно представляет интерес для любого соседнего транспортного средства, но конфиденциальность очень важна, когда транспортные средства делятся своей позицией. В текущих стандартах ИТС используются псевдонимы, чтобы затруднить отслеживание местоположения транспортного средства

внешними объектами и защитить его личность. Транспортным средствам выдаётся несколько «несвязанных» псевдонимных сертификатов, которые при определённых обстоятельствах, например, плохо управляемые автомобили, могут быть полностью отозваны с помощью управляемой дорожной инфраструктуры. Хотя использование этих псевдонимных сертификатов необходимо для защиты конфиденциальности, этого недостаточно: все другие идентификаторы протокола, например, MAC-адрес, порядковые номера, IP-адреса, порты и т.д., также должны быть изменены соответствующим образом. Более того, все ещё существует проблема RF-отпечатка [3], который может идентифицировать радиоизлучатель, даже если все идентификаторы удалены.

Внедрение технологии DLT в V2X

Увеличение объёма информации в транспортных средствах следующего поколения также потребует новых механизмов для обеспечения целостности и подлинности всех данных о транспортных средствах, а также соблюдения требований конфиденциальности. Децентрализованный характер этой информации и тот факт, что вождение автомобиля основано в основном на общедоступных данных, обеспечивают некоторые основы для подхода к ИТС с помощью блокчейна с целью предоставления открытой, прозрачной и безопасной децентрализованной платформы ИТС.

Одна из первых работ, посвящённых вопросам ИТС с использованием технологий блокчейн, датируется 2016 годом. В [4] авторы представляют предварительное исследование ИТС на основе блокчейн. Работа носит в основном концептуальный характер, хотя они представляют собой тематическое исследование для сервисов совместного использования поездок в реальном времени на основе блокчейнов. Другие авторы в [5] пытаются объединить транспортные сети Ad-hoc (VANET) и концепции приложений на основе блокчейна Ethereum, чтобы обеспечить прозрачные, самоуправляемые и децентрализованные сервисы ИТС без необходимости в центральном управляющем органе. Эта работа в основном сосредоточена на регулировании дорожного движения, налогообложении транспортных средств и страховании транспортных средств. В [6] блокчейн используется для предотвращения мошенничества с одометрами при сохранении принципов конфиденциальности. Записи хранятся в зашифрованном виде во внутреннем хранилище, а блокчейн используется для предотвращения подделки зашифрованных записей. Предотвращение мошенничества с одометром является типичным вариантом использования блокчейна [7] и послужило основой для различных прототипов Proof-of-Concept [8]. На рынке уже есть решение в этой линейке: VinChain 1. В [9] авторы предлагают использовать блокчейн для реализации системы страховых записей, которая может включать все аспекты страховых транзакций. В [10] авторы предлагают использовать технологию блокчейн для формирования автомобильной цепочки блоков, которая выполняет распределенное хранение данных и безопасный обмен данными. Однако этот подход не касается управления сетью — реальной проблемой для развёртывания ИТС. В последнее время появились предложения использовать блокчейн для передачи данных в парадигме Интернета транспортных средств (IoV). В [11] авторы предлагают гибридную архитектуру блокчейна и машинное обучение для выбора узлов. В [12] предлагается использование глубокого машинного обучения для реализации интеллектуального кэширования данных с использованием блокчейна в Vehicle Edge Computing (VEC).

Проблемы внедрения

Общей проблемой для всех подходов к ИТС является обеспечение связи V2X. В зависимости от приложения могут использоваться разные технологии, поскольку не все из них имеют один и тот же критичный диапазон по времени. Например, для подключённой информационной службы светофора требования к максимальной задержке менее строгие, чем для приложений V2V, таких как совместное смягчение движения или предотвращение столкновений или адаптивный круиз-контроль, где несколько дополнительных миллисекунд могут быть разницей между столкновением с автокатастрофой или её предотвращением. Как правило, они не критичны по времени, если их можно реализовать с помощью обычные сети 4G / LTE [13], т.е. с максимальной задержкой более 100 мс. Некоторые автопроизводители уже предоставляют услуги ИТС, используя сотовую связь вместо прямой связи I2V. Например, Audi запустила Audi Traffic Light Information в Лас-Вегасе в 2016 году и начала тестировать её в Европе в 2019 году с целью внедрения Time-to-Green во всех автомобилях. Чтобы получить доступ к этой услуге, у вас должен быть автомобиль Audi, совместимый с их услугой подписки, тогда как при использовании прямой связи информацию получит любой автомобиль, находящийся достаточно близко. Используя прямую связь, система не зависит исключительно от сотовой сети. С другой стороны, прямая связь в соответствии с действующими стандартами ИТС потребует установки специального оборудования в автомобиле.

Для массового внедрения коммуникаций V2X нам нужна широко распространённая и доступная по цене технология. 5G обещает стать фактором поддержки V2X, но до тех пор, пока 5G не получит широкого глобального распространения, стоимость этой технологии будет препятствием. Если мы попытаемся найти технологию связи ближнего действия, уже широко использующуюся

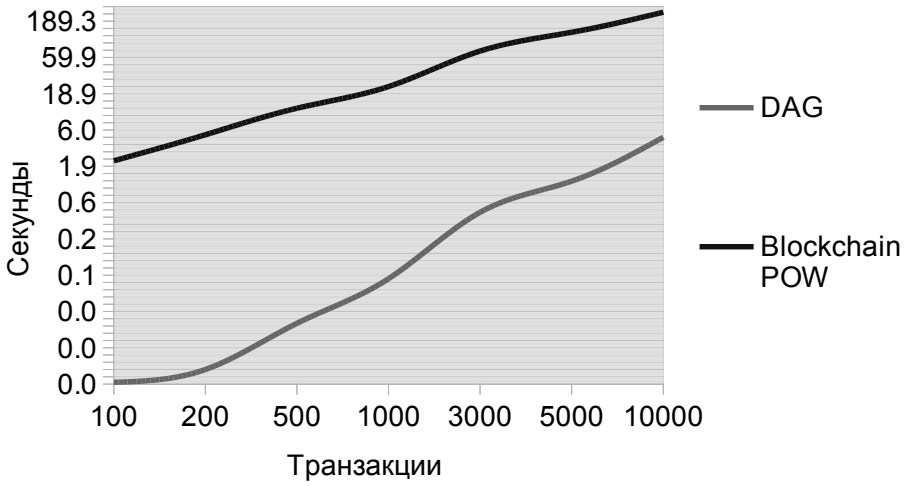

Рис. 1. Зависимость транзакции от времени

по доступной цене, и там, где любое устройство может общаться с любым устройством, находящимся поблизости — Bluetooth Low Energy — единственный выбор. Согласно обновлению рынка Bluetooth за 2019 год [14], более 3 миллиардов устройств Bluetooth были поставлены с поддержкой Bluetooth Low Energy. Все смартфоны, выпущенные в 2019 году, включали Bluetooth, большинство из них с Bluetooth Low Energy. Что касается операционных систем, то наиболее представительные, то есть iOS и Android, поддерживает Bluetooth Low Energy с 2013 года, расширяя сценарии использования Bluetooth, от услуг на основе определения местоположения [15] до IoT [16]. Некоторые авторы даже проанализировали пригодность BLE для критичных по времени промышленных приложений IoT [17]. Несмотря на то, что ранее предпринимались попытки реализовать услуги ИТС через Bluetooth Low Energy [18], она опирается на уменьшенную модель безопасности из-за ограничения, наложенного в BLE4.0 на широковещательные сообщения, т.е. 31 байт.

Блокчейн на основе ориентированного ациклического графа

Так как V2X по сути своей это разновидность IoT, то для внедрения технологии распределенных реестров (DLT) необходимо учитывать некоторые ограничения и требования [19], относящиеся к инфраструктуре Io T. Поэтому предлагается использовать в V2X блокчейн на основе ориентированного ациклического графа [19]. В ходе данного исследования был разработан прототип, моделериующий создание и обработку большого количества сообщений. Моделируется создание двух блокчейнов: традиционного с майниногом и на основе графа без майнинга. Результаты моделирования можно посмотреть на Рис. 1, где изображена зависимость количества транзакций от времени. Однако, стоит отметить, что на данный момент в версии с графом отсутствует механизм консенсуса, что должно снизить эффективность, но концептуально такой подход по-прежнему остаётся предпочтительным в IoT, за счёт скорости обработки сообщений.

Заключение

Одним из основных препятствий для массового внедрения этих технологий является управление. Текущие решения основаны на использовании инфраструктуры с открытым крипто-ключом, которая обеспечивает безопасное сотрудничество между различными объектами в экосистеме V2X, но, учитывая глобальный масштаб, управление такой инфраструктурой требует заключения соглашений между многими сторонами, что приводит к конфликту интересов между автопроизводителями и операторами электросвязи. В результате доступно множество вариантов использования и две зрелые коммуникационные технологии, но сложность на бизнес-уровне не позволяет драйверам использовать преимущества приложений ИТС. Технологии блокчейн определяют новую парадигму децентрализации для большинства традиционных приложений, в которой смарт-контракты обеспечивают простой механизм децентрализованного управления. В этой работе предлагается подход для децентрализованного V2X (D-V2X), который не требует никаких доверенных полномочий и может быть реализован поверх любого протокола связи. Технология для D-V2X готова к применению, и уже существуют аппаратные платформы, способные ее запустить. D-V2X может

не заменить отраслевые стандарты в краткосрочной перспективе, но, как часть усилий сообщества, некоторые дополнительные услуги могут быть реализованы через D-V2X. Такие технологии, как DID и VC, могут обеспечить полностью децентрализованную инфраструктуру идентификации для приложений ИТС. Чтобы иметь полностью децентрализованную среду, любой должен иметь доступ к этой технологии. Необходимо устранить технологические барьеры, поэтому некоторые варианты использования ИТС могут быть реализованы с использованием BLE — широко распространённой технологии, уже присутствующей во всех современных смартфонах и транспортных средствах. Основная проблема, с которой мы сейчас сталкиваемся,— это как оптимизировать соединение с блокчейном как для транспортных средств, так и для участников дорожного движения. В качестве дальнейшего исследования планируется разработать блокчейн на основе ациклического графа, что может помочь устранить проблему со сложностью соединения блокчейна и дорожной инфраструктуры, за счёт уменьшенного времени обработки транзакции и древовидной архитектуры цепочек.

ЛИТЕРАТУРА

1. S.E. Shladover, “Connected and automated vehicle systems: Introduction and overview,” Journal of Intelligent Transportation Systems, vol. 22, no. 3, pp. 190–200, 2018.
2. A. Ghosal and M. Conti, “Security issues and challenges in V2X: A Survey,” Computer Networks, vol. 169, no. 107093, pp. 1–20, 2020.
3. B. Danev, D. Zanetti, and S. Capkun, “On physical-layer identification of wireless devices,” ACM Comput. Surv., vol. 45, no. 1, Dec. 2012.
4. Y. Yuan and F. Wang, “Towards blockchain-based intelligent transportation systems,” in 2016 IEEE19th International Conference on Intelligent Transportation Systems (ITSC), 2016, pp. 2663–2668.
5. B. Leiding, P. Memarmoshrefi, and D. Hogrefe, “Self-managed and blockchain-based vehicular ad-hoc networks,” in Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct, ser. UbiComp ’16. New York, NY, USA: Association for Computing Machinery, 2016, pp. 137–140.
6. M. Chanson, A. Bogner, F. Wortmann, and E. Fleisch, “Blockchain as a privacy enabler: An odometer fraud prevention system,” in Proceedings of the 2017 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2017 ACM International Symposium on Wearable Computers, ser. UbiComp ’17. New York, NY, USA: Association for Computing Machinery, 2017, pp. 13—-16.
7. P. Fraga-Lamas and T.M. Fernández-Caramés, “A review on blockchain technologies for an advanced and cyber-resilient automotive industry,” IEEE Access, vol. 7, pp. 17 578–17 598, 2019.
8. L.R. Abbade, F.M. Ribeiro, M.H. d. Silva, A.F.P. Morais, E.S. d. Morais, E.M. Lopes, A.M. Alberti, and J.J. P.C. Rodrigues, “Blockchain applied to vehicular odometers,” IEEE Network, vol. 34, no. 1, pp. 62–68, 2020.
9. M. Demir, O. Turetken, and A. Ferworn, “Blockchain based transparent vehicle insurance management,” in 2019 Sixth International Conference on Software Defined Systems (SDS), 2019, pp. 213–220.
10. J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, “Blockchain for secure and efficient data sharing in vehicular edge computing and networks,” IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4660–4670, 2019.
11. Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, “Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles,” IEEE Transactions on Vehicular Technology, vol. 69, no. 4, pp. 4298–4311, 2020.
12. Y. Dai, D. Xu, K. Zhang, S. Maharjan, and Y. Zhang, “Deep rein forcement learning and permissioned blockchain for content caching in vehicular edge computing and networks,” IEEE Transactions on Vehicular Technology, vol. 69, no. 4, pp. 4312–4324, 2020.
13. Z. Xu, X. Li, X. Zhao, M. Zhang, and Z. Wang, “Dsrc versus 4g-lte for connected vehicle applications: A study on field experiments of vehicular communication performance,” Journal of advanced transportation, vol. 435, Aug. 2017.
14. Bluetooth SIG, Inc.,“Bluetooth market update 2019,” 2019, https://www.bluetooth.com/bluetooth-resources/2019-bluetooth-market-update/.
15. R. Faragher and R. Harle, “Location fingerprinting with bluetooth low energy beacons,” IEEE journal on Selected Areas in Communications, vol. 33, no. 11, pp. 2418–2428, 2015.
16. J. Fürst, K. Chen, H.-S. Kim, and P. Bonnet, “Evaluating bluetooth low energy for IoT,” in 2018 IEEE Workshop on Benchmarking Cyber Physical Networks and Systems (CPSBench). IEEE, 2018, pp. 1–6.
17. R. Rondón, M. Gidlund, and K. Landernäs, “Evaluating bluetooth low energy suitability for time-critical industrial IoT applications,” Interna tional Journal of Wireless Information Networks, vol. 24, no. 3, pp. 278–290, 2017.
18. K. Thomas, H. Fouchal, S. Cormier, and F. Rousseaux, “Intelligent transport system based on bluetooth,” in International Workshop on Communication Technologies for Vehicles. Springer, 2019, pp. 50–59.
19. Салагаев А.А., Молодяков С.А. Внедрение технологии распределенного реестра в инфраструктуру IoT // XXIII Международная конференция по мягким вычислениям и измерениям (SCM-2020). Сборник докладов. СПб. 27–29 мая 2020 г. С.163–165

Журнал «Современная наука: актуальные проблемы теории и практики»