УДК 004.62:004.056.5

ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ ДОКУМЕНТООБОРОТА ЧЕРЕЗ ГИБРИДНЫЙ БЛОКЧЕЙН И ИЗОЛИРОВАННОЕ ИСПОЛНЕНИЕ КОДА

В.Л. Мальцев, С.А. Олексин, А.И. Самосюк
Учреждение образования «Национальный детский технопарк», г. Минск, Республика Беларусь

Аннотация. В статье рассматривается система электронного документооборота на основе гибридного блокчейна и изолированного исполнения кода в виртуальной машине XVM. Неделимые токены (NFT) фиксируют хеши документов, разграничение ролей реализовано на уровне байт-кода. Детерминизм и криптографическая проверка целостности, дополненные изоляцией исполнения, обеспечивают пригодность системы для юридически значимого документооборота, гарантируя неизменяемость записей и повышая надежность хранения.
Ключевые слова: гибридный блокчейн; электронный документооборот; целостность данных; изолированное исполнение кода; виртуальная машина; песочница; неделимый токен; NFT; криптографическая подпись; детерминизм.

PROVIDING DOCUMENT FLOW VIA A HYBRID CABLE AND ISOLATED CODE EXECUTION

V. Maltsau, S. Aleksin, A. Samasiuk
Educational Institution "National Children's Technopark", Minsk, Republic of Belarus

Abstract. The paper considers an electronic document management system based on hybrid blockchain and isolated code execution in the XVM virtual machine. Non-fungible tokens (NFTs) record document hashes, role-based access control is implemented at the bytecode level. Determinism and cryptographic integrity verification, complemented by execution isolation, make the system suitable for legally significant document workflows, ensuring immutability of records and enhancing storage reliability.
Keywords: hybrid blockchain; electronic document management; data integrity; isolated code execution; virtual machine; sandbox; non-fungible token; NFT; digital signature; determinism.

Введение

Электронный документооборот и количество подписей с помощью ЭЦП неуклонно растут, вытесняя бумагу. Однако остается открытым вопрос о достаточности существующих инструментов для обеспечения надежности и безопасности такого перехода. Большой популярностью пользуются централизованные системы провайдеров, однако они имеют ряд недостатков. Один из главных – отсутствие гарантии неизменяемости действий и недостаточно гибкая система разграничения прав доступа.

Основная часть

Предлагаемое решение использует гибридный блокчейн, сочетающий неизменяемость данных, криптографическую защиту и тонкое управление доступом. Участники разделены на уровни прав (типы кошельков A–D). Цифровым представлением документов служат неделимые токены (NFT), в метаданных которых хранятся хеш документа, адрес владельца, срок действия и иные сведения. NFT не является подлинником, но доказывает существование документа и историю операций; после истечения срока или отмены токен сжигается, а записи о всех операциях навсегда сохраняются в блокчейне.

Ядро системы – виртуальная машина XVM (eXtended Virtual Machine) с изолированным исполнением кода. XVM построена по стековому принципу, включает стек данных, стек вызовов, глобальную память и динамическую кучу. Детерминизм (одинаковый результат на любом узле) достигается фиксированным набором из 63 опкодов и отсутствием недетерминированных системных вызовов. Изоляция реализована через классическую «песочницу»: код не может напрямую обращаться к файловой системе, сети или памяти других процессов; взаимодействие с внешней средой возможно только через контролируемые системные вызовы. Среда исполнения отслеживает потребление ресурсов, прерывая выполнение при превышении лимита инструкций, что предотвращает DoS-атаки.

Проверка прав доступа встроена в интерпретатор байт-кода: роль пользователя хранится в структуре кошелька, и при попытке привилегированного действия анализ роли выполняется до обработки остальных инструкций. Криптографические операции (SHA-512, генерация ключей Ed25519) реализованы нативными опкодами, передающими данные в высокопроизводительные модули хост-системы, что сохраняет атомарность и обеспечивает высокую скорость обработки транзакций.

Процесс работы с документами строится на неизменяемых записях в реестре. При выпуске документа формируется транзакция создания NFT, фиксирующая 512-битный хеш файла, идентификатор владельца, временную метку и статус. Транзакция подписывается закрытым ключом эмитента и упаковывается в блок. Передача прав инициируется текущим владельцем: в транзакции указываются идентификатор NFT и адрес нового владельца, XVM проверяет право и обновляет запись, сохраняя полную

хронологию. Даже при «сжигании» документа все предыдущие записи остаются нетронутыми.

Такая архитектура меняет модель доверия: администратор не может скрыто изменить записи – попытка модификации нарушает хеш-связку блоков, что обнаруживается функцией периодической проверки целостности. Это обеспечивает невозможность отказа от авторства и доказуемую целостность истории, что критически важно для юридически значимых документов.

Блокчейн развернут как сеть взаимодействующих серверов с дублированием данных. Любое действие подтверждается подписью транзакции, буферный сервер проверяет подпись и передает запрос основному серверу. Основной набор команд включает создание, передачу и уничтожение NFT, управление кошельками, информационные запросы. Для расширения функционала предусмотрена возможность создания модулей на языке xLang (C-подобный язык со встроенными криптофункциями), работающих внутри песочницы.

Предлагаемая система сочетает высокую безопасность, прозрачность и гибкость, что делает ее перспективным решением для задач, требующих гарантированной достоверности данных.

Заключение

Предложенная архитектура электронного документооборота на основе гибридного блокчейна и изолированного исполнения кода обеспечивает криптографическую подтверждаемость операций, неизменяемость данных и защиту от несанкционированной модификации, что делает ее пригодной для юридически значимого документооборота. Предложенная архитектура масштабируема и адаптируема за счет возможности расширения функционала модулями на языке xLang, что открывает перспективы для внедрения системы в организациях с высокими требованиями к достоверности и прозрачности документооборота.

Список использованных источников

1. Конорев, Н., С. Мазуров, С. Перспективы применения технологии блокчейн в Республике Беларусь. – Минск: жур. «Банкаўскі веснік», разд. Цифровые технологии – 2000-2025. – с. 66-71.

2. Косба А., Миллер А., Ши Э., Вэнь З., Папаманту К. Hawk: модель криптографии с сохранением конфиденциальности для блокчейна и смарт-контрактов // 2016 IEEE Symposium on Security and Privacy (SP). – 2016. – С. 839–858.

References

1. Konorev N., Mazurov S. Prospects for the application of home lighting technologies in the Republic of Belarus // Bankauski vesnik. – 2025. – P. 66–71. (in Russian).

2. Kosba A., Miller A., Shi E., Wen Z., Papamanthou C. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts // 2016 IEEE Symposium on Security and Privacy (SP). – 2016. – P. 839–858.

Сведения об авторах

Мальцев В.Л. – заведующий лабораторией «Информационная безопасность» учреждения образования «Национальный детский технопарк», viktor.maltsevlul@gmail.com.

Олексин С.А. – учащийся учреждения образования «Национальный детский технопарк», г. Минск, Республика Беларусь, e-mail: simonoleksin@gmail.com.

Самосюк А.И. – учащийся учреждения образования «Национальный детский технопарк», г. Минск, Республика Беларусь, e-mail: sasha20ahsas@gmail.com.

Information about the authors

Maltsau V. – Head of the Information Security Laboratory, Educational Institution "National Children's Technopark", viktor.maltsevlul@gmail.com.

Aleksin S. – student Educational Institution "National Children's Technopark", simonoleksin@gmail.com.

Samasiuk A. – student, Educational Institution "National Children's Technopark", Sasha20ahsas@gmail.com.