

## ОРГАНИЗАЦИЯ КИБЕРФИЗИЧЕСКИХ ПРОИЗВОДСТВЕННЫХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ БЛОКЧЕЙН И СМАРТ-КОНТРАКТОВ

М. Я. АФАНАСЬЕВ, Ю. В. ФЕДОСОВ, А. А. КРЫЛОВА, С. А. ШОРОХОВ

*Университет ИТМО, 197101, Санкт-Петербург, Россия*

*E-mail: stratumxspb@gmail.com*

Рассматривается базовая распределенная сеть киберфизической производственной системы на основе частного блокчейна Ethereum. Приводится описание структуры сети и взаимодействие сетевых узлов через исполнение смарт-контрактов.

**Ключевые слова:** блокчейн, киберфизические системы, распределенная сеть, смарт-контракт, производственная система, управление, взаимодействие узлов сети

Понятие „блокчейн“ получило широкую известность в 2009 г. с появлением криптовалюты Bitcoin, и относительно недавно начали обсуждаться перспективы применения блокчейна в других областях. Блокчейн — это технология хранения и обработки данных в виде цепочки блоков в компьютерных сетях, не относящаяся ни к одному конкретному домену [1]. Каждый блок в цепочке может содержать произвольные данные, в том числе о процессах производства, что позволяет описать возможности применения этой технологии в производственных системах [2].

Разработка киберфизических производственных систем (КФПС) и промышленного интернета вещей требует решения многих проблем, связанных с обменом и обработкой данных: хранением, доступом, безопасностью и т.д. Более того, в настоящее время существует тенденция к созданию распределенных систем вместо централизованных. Одним из важнейших свойств интернета вещей является автономность его узлов и их способность взаимодействовать друг с другом [3]. Данный тип взаимодействия основан на концепции обслуживания, когда определенные узлы предоставляют сервисы другим узлам сети. Для обеспечения подобного взаимодействия некоторые реализации блочной цепи имеют специальный механизм смарт-контрактов.

*Смарт-контракт* — это самоисполняющийся сценарий, который хранится в блокчейне наряду с другими данными. Каждый смарт-контракт имеет определенный алгоритм, реализованный на специализированном языке программирования, что позволяет совершать любые действия автоматически без привлечения третьих лиц. Смарт-контракт контролирует выполнение определенных условий и принимает решения на их основе в соответствии с описанным алгоритмом. Поскольку подписать контракт может любой участник сети, этот способ взаимодействия применим к узлам сети интернета вещей. Данный механизм позволяет обеспечить надежную среду для взаимодействия узлов в сети и сделать предоставление сервисов прозрачным и унифицированным. Более того, нет необходимости создавать отдельный реестр сервисов, поскольку все контракты уже хранятся в блокчейне [4].

Очевидно, что технология блокчейн является достаточно универсальной; на сегодняшний день существует огромное число ее реализаций, используемых в разных областях человеческой деятельности [5, 6]. Для того чтобы эффективно использовать все преимущества технологии блокчейн для построения КФПС и промышленного интернета вещей, необходимо

разработать оптимальную с точки зрения решаемых задач структуру сети блокчейн и выбрать наиболее подходящие инструментальные средства (программные и аппаратные).

Основной отличительной особенностью КФПС является практически полная „прозрачность“ связей между физическими и логическими компонентами системы. Можно сказать, что в киберфизической системе стирается грань между реальными и виртуальными компонентами [7]. В противоположность этому в традиционных промышленных сетях основной акцент делается на физические устройства — программируемые логические контроллеры (ПЛК). В соответствии с этой концепцией только ПЛК осуществляют вычисления в сети, а также отвечают за надлежащее исполнение технологического процесса и информационное взаимодействие модулей промышленного оборудования. При этом четко разделены понятия „информационный поток“ и „материальный поток“.

Следует упомянуть также о неполном соответствии используемых промышленных протоколов требованиям, предъявляемым к современным информационным и телекоммуникационным технологиям. Например, в широко распространенном промышленном протоколе „Modbus“, несмотря на его открытость, используются методы, характерные для 70-х годов прошлого века, которые производители пытаются усовершенствовать за счет использования современных транспортных протоколов, что представляется крайне нерациональным подходом [8]. Также нельзя не отметить, что понятие „кибербезопасность“ в принципе не применимо ко многим ныне используемым промышленным стандартам, опять же вследствие их значительного отставания от современных информационных и телекоммуникационных технологий.

Переходя к сравнению промышленных сетей с индустриальным интернетом вещей, вначале следует обратиться к общему определению интернета вещей. К сожалению, авторам не удалось найти ни одного промышленного или иного стандарта, в перечне терминов которого присутствовало бы определение понятия „Интернет вещей“, но на основании проанализированной литературы можно дать следующую общую формулировку данного термина: „Интернет вещей — это вычислительная сеть, состоящая из физических устройств, оснащенных встроенной электроникой (и программным обеспечением), датчиками, исполнительными механизмами и средствами связи, которые позволяют этим устройствам общаться между собой и обмениваться данными“.

Подобное определение кажется похожим на определение понятия „киберфизическая система“, однако между ними есть одно существенное отличие. Промышленный интернет вещей не предназначен для выполнения какой-то определенной общей цели и, таким образом, не является системой в классическом ее понимании. Необходимо отметить, что КФПС — это холоническая система [9], т.е. состоящая из набора „физических сущностей“ и их „виртуальных двойников“, соединенных воедино. „Виртуальный двойник“ представляет собой вычислительную модель „физической сущности“, т.е. воспроизводит поведение физической машины и дает представление о том, как эта машина реагирует на появление различных внешних воздействий. Соединение может быть выполнено с помощью датчиков и исполнительных механизмов.

Холоническая природа КФПС подразумевает наличие как иерархических, так и гетерархических связей, что означает возможность их объединения во временные сущности более высокого порядка, т.е. „систему систем“. При этом все связи осуществляются через общую и открытую для всех участников сеть, которая и является интернетом вещей или индустриальным интернетом вещей. Таким образом, КФПС формирует первый уровень, а интернет вещей — второй уровень вертикальной цифровой интеграции.

Очевидно, что используемые стандарты промышленных сетей на основе ПЛК даже по совокупности свойств не могут считаться ни киберфизическими промышленными системами, ни индустриальным интернетом вещей. Последнее утверждение обусловливается тем, что

подобные сети не являются протокол-ориентированным или сервис-ориентированным решениями, характеризуются четким разделением материальных и информационных потоков, не имеют в своем составе аналогов „виртуальных двойников“, а также обладают жесткой иерархической системой управления с единым центром, не предполагающей наличия гетерархических связей и возможности гибкого перестроения.

Необходимо отметить, что проблема устаревания промышленных протоколов появилась уже достаточно давно. Еще в 1996 г. организацией OPC Foundation было разработано семейство протоколов Open Platform Communications (OPC), призванных стать основной технологией и предоставляющих единый интерфейс для управления объектами автоматизации и технологическими процессами. Более перспективным представляется логическое развитие протокола OPC, именуемое OPC Unified Architecture (OPC UA). Данная спецификация определяет передачу данных в промышленных сетях и взаимодействие устройств в них. Основными достоинствами подобного подхода являются открытость, независимость от какой-либо конкретной операционной системы или технологии, масштабируемость, реализация собственной системы обеспечения кибербезопасности. Однако, как и любая другая спецификация, создаваемая как промышленный стандарт, OPC UA не лишена определенных недостатков. OPC UA ориентирована на промышленные ПЛК и является достаточно сложным протоколом, который должен вместить в себя различные области промышленной автоматизации. Тем не менее на сегодняшний день OPC UA является самым проработанным протоколом и именно его решено взять за основу проектируемой архитектуры КФПС.

Итак, подробно рассмотрев понятия „промышленный интернет вещей“ и „киберфизические производственные системы“, можно перейти непосредственно к внедрению технологии блокчейн в их структуру.

Существуют два основных подкласса блокчейн-сетей — глобальные и частные. Первые являются наиболее развитыми и используются, как правило, для решения задач мирового масштаба. Глобальные пиринговые сети отличаются высокой стабильностью за счет большого количества участников, однако не подходят для создания сетей предприятия, аналогичных описанным выше промышленным сетям. При этом основным ограничением является жесткая привязка всех операций по обмену данными к криптовалюте, используемой в том или ином глобальном блокчейне. Прогнозировать изменение биржевых котировок на рынке криптовалют практически невозможно, что делает труднопредсказуемой стоимость владения проектируемой КФПС. Поэтому основу разрабатываемой архитектуры будет составлять частный блокчейн. Функциями блокчейна в КФПС должны стать:

- организация единого информационного пространства для межмашинного взаимодействия в рамках КФПС;
- обеспечение кибербезопасности КФПС;
- обеспечение легкого масштабирования и реструктуризации КФПС;
- обеспечение избыточности оборудования и каналов связи;
- организация единого хранилища данных;
- реализация технологии „цифровых двойников“ за счет использования смарт-контрактов;
- обеспечение выполнения общих для КФПС задач за счет использования смарт-контрактов.

Представленные требования существенно ограничивают выбор инструментальных средств, так как реализация ключевых функций КФПС подразумевает возможность работы со смарт-контрактами. На текущий момент смарт-контракты реализованы в нескольких частных блокчейн-сетях, однако только Ethereum обладает хорошо продуманной и отлаженной виртуальной машиной (Ethereum Virtual Machine — EVM), реализующей свой собственный полный по Тьюрингу язык программирования, наряду с возможностью работы со многими современ-

ными высокоуровневыми языками программирования посредством компиляции в байт-код EVM. Таким образом, в качестве основной платформы для построения КФПС будет использован частный блокчейн Ethereum.

Согласно представленному выше анализу, блокчейн, используемый в глобальных распределенных платежных системах, не подходит для создания опорной сети КФПС. Очевидно, что основным ограничением для применения данной технологии в неизменном виде является механизм обеспечения консенсуса при подтверждении транзакций, т.е. консенсусный протокол. В подавляющем большинстве пиринговых платежных систем используется так называемый консенсус Никамото, иначе именуемый „Proof of Work“ (доказательство работы). В соответствии с данным алгоритмом для предотвращения злоупотребления услугами распределенной сети запрашивающая сторона должна выполнить определенную достаточно сложную вычислительную работу, результат которой быстро проверяется обслуживающей стороной. Это означает, что узлы сети КФПС должны обладать достаточной мощностью, чтобы выполнять работу по генерации новых блоков.

Также необходимо отметить, что на текущий момент наиболее развитыми и технологически зрелыми являются блокчейн-сети глобального масштаба, в частности сети международных пиринговых платежных систем, наподобие Bitcoin, Litecoin, Ethereum и т.д., однако их прямое использование в качестве опорной сети КФПС не представляется возможным по целому ряду причин.

Во-первых, лишь некоторые глобальные сети имеют возможность работать со смарт-контрактами. На момент написания данной статьи основной сетью, предоставляющей сервис смарт-контрактов общего назначения, является Ethereum. Во-вторых, при выполнении смарт-контракта расходуется так называемый „газ“\*. Термин „расход газа“ используется для обозначения того, сколько „газа“ нужно, чтобы выполнить определенное действие на платформе. Цена „газа“ зависит от цены криптовалюты, т.е. при использовании данной технологии любой информационный обмен между узлами КФПС будет иметь определенную стоимость, причем она будет напрямую связана с ценой данной криптовалюты.

На основании вышесказанного можно сделать вывод, что несмотря на большие возможности глобальной сети Ethereum, в частности использование ее в качестве распределенного криптозащищенного облачного хранилища, применение данной технологии в КФПС экономически невыгодно [10, 11]. Однако анализ научных работ по практическому применению блокчейна показал, что эта технология остается эффективной даже в том случае, если используется в частной локальной сети предприятия.

Таким образом, было рассмотрено несколько вариантов архитектуры опорной сети.

1. Использование в качестве опорной сети технологии блокчейн, аналогичной применяемой в пиринговой платежной системе Bitcoin, только в приватном исполнении. В данном случае предполагается использование консенсусного протокола „Proof of Work“ с уменьшенной первоначальной сложностью генерации блока и выделение специализированных майнинговых ферм, обеспечивающих работоспособность сети. При этом рабочие узлы КФПС (датчики, оборудование и т.д.) не будут выполнять работу по генерации блоков, а также не будут хранить всю историю блокчейна начиная с первого блока. Вместо этого используется технология „тонких клиентов“, когда конечные узлы должны хранить только заголовки блоков.

Очевидным достоинством системы Bitcoin является ее широкое распространение. Bitcoin успешно применяется уже достаточно долго, исходный код клиента прошел многократные проверки не только участниками сообщества, но и экспертами в области информационной безопасности. Тем не менее не стоит забывать и о недостатках системы Bitcoin. Как было отмечено ранее, применительно к рассматриваемой предметной области критичным

---

\* Газ — здесь: единица вычислительной мощности в сети Ethereum.

требованием к сети блокчейн является исходная реализация смарт-контрактов. Bitcoin поддерживает смарт-контракты, однако используемый для их написания язык сценариев не является полным по Тьюрингу, что ставит под сомнение применение данной технологии для межмашинного взаимодействия и автоматизации производственных процессов в рамках КФПС.

2. Использование специализированного блокчейна, ориентированного на безопасное межмашинное взаимодействие в интернете вещей. Наиболее проработанным проектом в этой области является технология ИОТА. Транзакции в сети ИОТА бесплатны, так как весь объем используемой в данной системе криптовалюты был сгенерирован заранее. Время проведения транзакций значительно меньше, нежели в пиринговых платежных системах общего назначения, количество одновременных транзакций не ограничено. Система легко масштабируется и интегрируется с существующими КФПС.

Все это делает данную технологию крайне перспективной для использования в качестве опорной сети КФПС. Однако несмотря на перечисленные достоинства, данная технология не лишена и ряда существенных недостатков. Во-первых, сеть ИОТА является еще слишком молодой (проект был представлен в июне 2016 г.); во-вторых, в ИОТА до сих пор не реализованы смарт-контракты, что существенно усложняет ее использование именно в специализированной промышленной среде.

3. Использование частного блокчейна Ethereum в совокупности с консенсусным протоколом „Proof of Stake“ (доказательство участия) [12]. Этот метод позволяет определять вероятность формирования узлом очередного блока в блокчейне пропорционально доле, которую составляют принадлежащие этому блоку расчетные единицы криптовалюты от их общего количества. При использовании данного метода алгоритм формирования блока не зависит от мощности оборудования, но с большей вероятностью блок будет сформирован той учетной записью, текущий баланс которой больше. Последнее является главным достоинством данного варианта построения опорной сети КФПС. Также необходимо отметить, что, помимо этого, „Proof of Stake“ обладает большей устойчивостью к хакерским атакам, что, безусловно, положительно скажется на безопасности проектируемой КФПС.

По результатам оценки достоинств и недостатков рассмотренных вариантов архитектуры опорной сети КФПС было принято решение использовать последний вариант, т.е. за основу взят блокчейн Ethereum с подключенным консенсусным протоколом „Proof of Stake“ и включенной возможностью использования как толстых, так и тонких клиентов. При этом все узлы КФПС будут ранжированы в соответствии с их значимостью. Значимость будет определяться влиянием узла на производственный процесс.

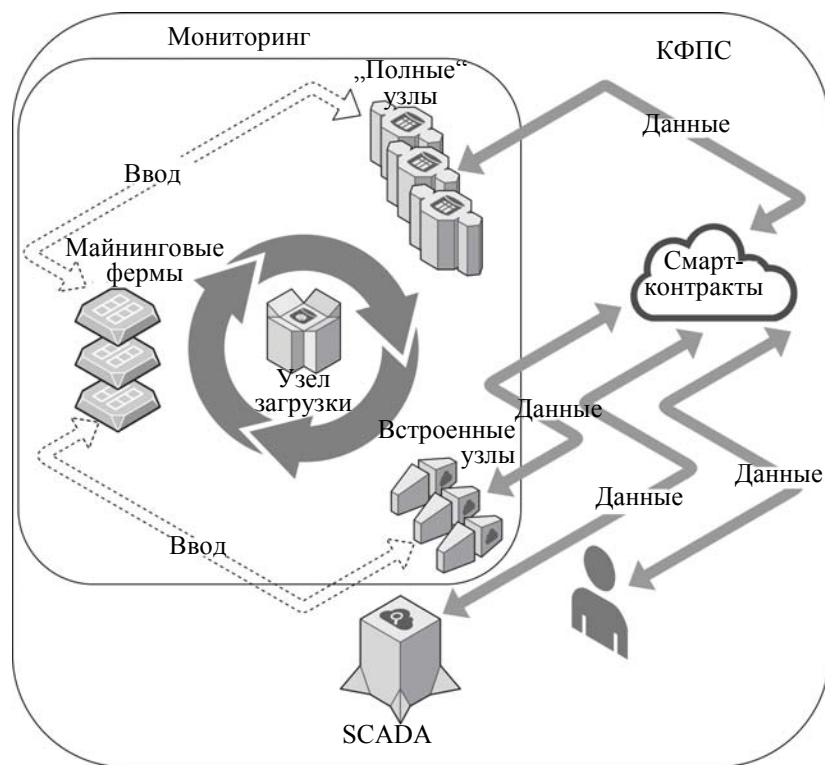
Например, станочное оборудование и промышленные роботы будут считаться „богатыми“ узлами, им будет выделено максимальное количество криптовалюты, за счет чего они получат мгновенный и беспрепятственный доступ ко всем ресурсам КФПС. Также будет выделен „средний класс“ — компоненты КФПС, относящиеся к планированию и логистике производственного процесса. Узлы, не имеющие прямого отношения к процессу производства, но необходимые для общего контроля и мониторинга, будут считаться „бедными“, им будет предоставлен ограниченный доступ к ресурсам. Например, датчики температуры и влажности в цехе являются „бедными“ узлами, так как нет необходимости регистрировать их показания слишком часто.

В рассматриваемом варианте именно смарт-контракты являются основой межмашинного взаимодействия (причем как между физическими компонентами КФПС, так и виртуальными). Смарт-контракты Ethereum представляют собой объекты, привязанные к аккаунту блокчейна. Они содержат исполняемый код и могут взаимодействовать с другими контрактами, принимать решения, хранить данные и отправлять криптовалюту другим узлам сети. Контракты определяются их создателями, но их исполнение, а также реализация предлагае-

мых услуг обеспечиваются самой сетью Ethereum. Контракты будут существовать и исполняться до тех пор, пока существует сеть в целом, и исчезнут, только если они запрограммированы на самоуничтожение.

В рассматриваемой архитектуре смарт-контракты используются для удаленного вызова процедур. В качестве основного языка программирования выбран „Solidity“, что обусловлено его широким распространением, схожестью с языком „JavaScript“, а также поддержкой статической типизации переменных и сложных структур [13].

Обмен данными в сети осуществляется по принципу „Publication-Subscribe“, подробно описанному в работах [9, 14]. Для хранения данных КФПС используется механизм „логов событий“ сети Ethereum. При этом общие для КФПС данные хранятся непосредственно в блокчейн-сети, тогда как „богатые“ узлы обладают собственным хранилищем, построенным на основе бессерверной нереляционной базы данных „UnQLite“ [15]. Таким образом, кэш данных хранится в базе данных, а непосредственно в блокчейне хранится скрипт загрузки базы данных из „логов событий“ Ethereum. Для конечных узлов используется клиент „geth“, для встраиваемых систем — специализированный тонкий клиент „EthEmbedded“.



Архитектура сети, основанная на частном блокчейне Ethereum и состоящая из узлов нескольких типов, представлена на рисунке. Узлы хранения и проверки данных, или так называемые „полные“ узлы, предназначены для хранения в памяти всех блоков с данными, кроме того, они могут выступать как инструмент для валидации блоков и генерации новых. Загрузочные узлы, как понятно из названия, служат для начальной загрузки сети, и каждый новый узел устанавливает соединение с ним для получения списка участников сети. Встроенные узлы выполняют роль связующего звена между непосредственно оборудованием и узлами загрузки, осуществляя контроль состояния сети. Помимо перечисленных, в сеть может быть также включен узел мониторинга для сбора статистики по сети: количество блоков, загрузка, транзакции и т.д, укомплектованный программным пакетом SCADA (Supervisory Control and Data Acquisition — диспетчерский контроль и сбор данных). Следует, однако, отметить, что представленная архитектура межмашинного взаимодействия в сети КФПС является прототипом и имеет ряд ограничений, так как в ней реализованы только базовые механизмы.

Безусловно, подобная система может быть расширена на счет введения новых компонентов. Однако добавление новых связей и формирование дополнительных информационных потоков может привести к значительному росту нагрузки на сеть, что негативно скажется на производительности КФПС. Не вызывает сомнений, что данный вопрос требует дополнительных исследований. Также следует отметить, что предлагаемый механизм взаимодействия узлов блокчейна ориентирован в первую очередь на общение „умных“ устройств, хотя блокчейн прекрасно подходит и для человекомашинного взаимодействия.

Исходя из концепции промышленного интернета вещей, можно отметить, что связь между устройствами распределенной производственной сети является важной особенностью КФПС. Поэтому необходимо обеспечить ее надежность, отказоустойчивость и безопасность исполнения. В роли такой среды для связи узлов может выступать технология блокчейн, обладающая механизмом работы смарт-контрактов. В настоящий момент определены правила работы описанного консенсусного протокола в сети установки. Текущие исследования направлены на внедрение физического прототипа на основе предложенного решения с использованием устройств интернета вещей.

Работа выполнена в рамках проекта 617026 „Технологии киберфизических систем: управление, вычисления, безопасность“.

#### СПИСОК ЛИТЕРАТУРЫ

1. Swan M. Blockchain: Blueprint for a New Economy. O'Reilly Media, 2015. P. 152.
2. Porru S., Pinna A., Marchesi M., Tonelli R. Blockchain-oriented software engineering: Challenges and new directions // Proc. of the 39th IEEE Intern. Conf. on Software Engineering Companion, Buenos Aires, Argentina. 2017. P. 169—171.
3. Teslya N., Ryabchikov I. Blockchain-based platform architecture for industrial IoT // Proc. of the 21st Conf. of Open Innovations Association FRUCT. 2017. P. 321—329.
4. Christidis K., Devetsikiotis M. Blockchains and smart contracts for the internet of things // IEEE Access. 2016. Vol. 4. P. 2292—2303.
5. Red V. A. Practical comparison of distributed ledger technologies for IoT // Proc. of SPIE. 2017. P. 6.
6. Daza V., Pietro R.D., Klimek I., Signorini M. CONNECT: CONTEXTual Name discovery for blockchain-based services in the IoT // IEEE ICC SAC Symposium Internet of Things Track, Paris, France. 2017.
7. Monostori L. Cyber-physical production systems: roots, expectations and R&D challenges // Procedia CIRP. 2014. Vol. 17. P. 9—13.
8. Thomas G. Introduction to Modbus serial and Modbus TCP // Contemporary Control Systems, Inc. 2008. Vol. 9. P. 4.
9. Afanasiev M. Y., Fedosov Y. V., Krylova A. A., Shorokhov S. A. An application of microservices architecture pattern to create a modular computer numerical control system // Proc. of the 20th Conf. of Open Innovations Association FRUCT. 2017. P. 10—19.
10. Xu Q., Aung K.M., Zhu Y., Yong K. L. A Blockchain-Based Storage System for Data Analytics in the Internet of Things. Springer Intern. Publ., 2018. P. 119—138.
11. Sharma P. K., Chen M.-Y., Park J. H. A software defined fog node based distributed blockchain cloud architecture for IoT // IEEE Access. 2017.
12. Biccifurri F., Lax G., Nicolazzo S., Nocera A. Overcoming limits of blockchain for IoT applications // Proc. of the 12th Intern. Conf. on Availability, Reliability and Security, Reggio di Calabria, Italy. 2017.
13. Dannen C. Introducing Ethereum and Solidity. Apress, 2017. P. 185.
14. Afanasiev M. Y., Fedosov Y. V., Krylova A. A., Shorokhov S. A. Performance evaluation of the message queue protocols to transfer binary JSON in a distributed CNC system // Proc. of the 15th IEEE Intern. Conf. on Industrial Informatics (INDIN), Emden, Germany. 2017. P. 357—362.

15. Afanasiev M. Y., Fedosov Y. V., Krylova A. A., Shorokhov S. A. Machine vision for selective polymer curing devices: Challenges and solutions // Proc. of the 21th Conf. of Open Innovations Association FRUCT. 2017. P. 391—397.

**Сведения об авторах**

- Максим Яковлевич Афанасьев** — канд. техн. наук, доцент; Университет ИТМО, кафедра технологии приборостроения; E-mail: amax@niuitmo.ru
- Юрий Валерьевич Федосов** — канд. техн. наук, доцент; Университет ИТМО, кафедра технологии приборостроения; E-mail: yf01@yandex.ru
- Анастасия Андреевна Крылова** — аспирант; Университет ИТМО, кафедра технологии приборостроения; инженер; E-mail: ananasn94@gmail.com
- Сергей Александрович Шорохов** — аспирант; Университет ИТМО, кафедра технологии приборостроения; инженер; E-mail: stratumxspb@gmail.com

Поступила в редакцию  
04.06.18 г.

**Ссылка для цитирования:** Афанасьев М. Я., Федосов Ю. В., Крылова А. А., Шорохов С. А. Организация киберфизических производственных систем с использованием технологий блокчейн и смарт-контрактов // Изв. вузов. Приборостроение. 2019. Т. 62, № 3. С. 226—234.

# ORGANIZATION OF CYBER-PHYSICAL PRODUCTION SYSTEMS USING BLOCKCHAIN AND SMART-CONTRACTS TECHNOLOGIES

M. Ya. Afanasiev, Yu. V. Fedosov, A. A. Krylova, S. A. Shorokhov

ITMO University, 197101, St. Petersburg, Russia  
E-mail: stratumxspb@gmail.com

The distributed network of a cyber-physical production systems based on the private blockchain system Ethereum is considered. A description of the network structure and the interaction of network nodes through the execution of smart-contracts is given.

**Keywords:** blockchain, cyber-physical systems, distributed network, smart-contract, production system, control, network nodes communication

**REFERENCES**

- Swan M. *Blockchain: Blueprint for a new economy*, O'Reilly Media, 2015, 152 p.
- Porru S., Pinna A., Marchesi M., Tonelli R. 2017 *IEEE/ACM 39th IEEE International Conference on Software Engineering Companion*, February, 2017, pp. 169–171.
- Teslya N., Ryabchikov I. *Proceedings of the 21st Conference of Open Innovations Association FRUCT*, 2017, pp. 321–329.
- Christidis K., Devetsikiotis M. *IEEE Access*, 2016, vol. 4, pp. 2292–2303.
- Red V.A. *Proceedings of SPIE*, 2017, pp. 6.
- Daza V., Pietro R.D., Klimek I., Signorini M. *IEEE ICC 2017 SAC Symposium Internet of Things Track*, 2017.
- Monostori L. *Procedia CIRP*, 2014, vol. 17, pp. 9–13.
- Thomas G. *Contemporary Control Systems*, Inc., 2008, vol. 9, p. 4.
- Afanasiev M.Y., Fedosov Y.V., Krylova A.A., Shorokhov S.A. *Proceedings of the 20th Conference of Open Innovations Association FRUCT*, 2017, pp. 10–19.
- Xu Q., Aung K.M., Zhu Y., Yong K.L. *A Blockchain-Based Storage System for Data Analytics in the Internet of Things*, Springer International Publishing, 2018, pp. 119–138.
- Sharma P.K., Chen M.-Y., Park J.H. *IEEE Access*, 2017.
- Biccafurri F., Lax G., Nicolazzo S., Nocera A. *ARES 2017 Proceedings of the 12th International Conference on Availability, Reliability and Security*, 2017.
- Dannen C. *Introducing Ethereum and Solidity*, Apress, 2017, 185 p.
- Afanasiev M.Y., Fedosov Y.V., Krylova A.A., Shorokhov S.A. *Proceedings of 2017 15th IEEE International Conference on Industrial Informatics (INDIN)*, 2017, pp. 357–362.
- Afanasiev M.Y., Fedosov Y.V., Krylova A.A., Shorokhov S.A. *Proceedings of the 21th Conference of Open Innovations Association FRUCT*, 2017, pp. 391–397.

**Data on authors**

- Maxim Ya. Afanasiev** — PhD, Associate Professor; ITMO University, Department of Instrumentation Technologies; E-mail: amax@niuitmo.ru
- Yuriy V. Fedosov** — PhD, Associate Professor; ITMO University, Department of Instrumentation Technologies; E-mail: yf01@yandex.ru



- Anastasia A. Krylova** — Post-Graduate Student; ITMO University, Department of Instrumentation Technologies; Engineer; E-mail: ananasn94@gmail.com
- Sergey A. Shorokhov** — Post-Graduate Student; ITMO University, Department of Instrumentation Technologies; Engineer; E-mail: stratumxspb@gmail.com

**For citation:** Afanasiev M. Ya., Fedosov Yu. V., Krylova A. A., Shorokhov S. A. Organization of cyber-physical production systems using blockchain and smart-contracts technologies. *Journal of Instrument Engineering*. 2019. Vol. 62, N 3. P. 226—234 (in Russian).

DOI: 10.17586/0021-3454-2019-62-3-226-234