О разрешительных принципах регулирования блокчейн и криптовалют в Республике Беларусь и подходах к созданию блокчейн платформ

Владимир Комисаренко, заместитель директора по развитию проектов в сфере защиты информации

LWO

Декрет Президента Республики Беларусь № 8 «О развитии цифровой экономики»

2. Создать условия для внедрения в экономику Республики Беларусь технологии реестра блоков транзакций (блокчейн)*, иных технологий, основанных на принципах распределенности, децентрализации и безопасности совершаемых с их использованием операций. С учетом того, что до принятия настоящего Декрета обращение цифровых знаков (токенов) (далее – токен) не было урегулировано законодательством и, соответственно, они не являлись объектом правоотношений, установить, что:

1. Оператор криптоплатформы – резидент Парка высоких технологий, предоставляющий с использованием информационной системы физическим и (или) юридическим лицам, в том числе нерезидентам Республики Беларусь, возможность совершения между собой и (или) с оператором криптоплатформы следующих сделок (операций):

отчуждение, приобретение цифровых знаков (токенов) за белорусские рубли, иностранную валюту, электронные деньги;

обмен цифровых знаков (токенов) одного вида на цифровые знаки (токены) другого вида;

иных сделок (операций) в соответствии с требованиями настоящего Декрета.

2. Виртуальный кошелек.

3. Владелец цифрового знака (токена).

4. Криптовалюта – биткоин, иной цифровой знак (токен), используемый в международном обороте в качестве универсального средства обмена.

5. Майнинг.

6. Оператор обмена криптовалют.

7. Размещение цифровых знаков (токенов).

8. Реестр блоков транзакций (блокчейн) – выстроенная на основе заданных алгоритмов в распределенной децентрализованной информационной системе, использующей криптографические методы защиты информации, последовательность блоков с информацией о совершенных в такой системе операциях.

9. Смарт-контракт.

12. Цифровой знак (токен) – запись в реестре блоков транзакций (блокчейне), иной распределенной информационной системе, которая удостоверяет наличие у владельца цифрового знака (токена) прав на объекты гражданских прав и (или) является криптовалютой.

2.1. юридические лица вправе владеть токенами и с учетом особенностей, установленных настоящим Декретом, совершать следующие операции:

через резидента Парка высоких технологий, осуществляющего соответствующий вид деятельности, создавать и размещать собственные токены в Республике Беларусь и за рубежом;

хранить токены в виртуальных кошельках;

через операторов криптоплатформ, операторов обмена криптовалют, иных резидентов Парка высоких технологий, осуществляющих соответствующий вид деятельности, приобретать, отчуждать токены, совершать с ними иные сделки (операции).

2.2. физические лица вправе владеть токенами и с учетом особенностей, установленных настоящим Декретом, совершать следующие операции: майнинг, хранение токенов в виртуальных кошельках, обмен токенов на иные токены, их приобретение, отчуждение за белорусские рубли, иностранную валюту, электронные деньги, а также дарить и завещать токены.

Деятельность по майнингу, приобретению, отчуждению токенов, осуществляемая физическими лицами самостоятельно без привлечения иных физических лиц по трудовым и (или) гражданско-правовым договорам, не является предпринимательской деятельностью. Токены не подлежат декларированию.

2.3. операторы криптоплатформ, операторы обмена криптовалют обязаны обеспечивать наличие на счетах в банках Республики Беларусь денежных средств в размере не менее 1 млн. белорусских рублей для оператора криптоплатформы, не менее 200 тыс. белорусских рублей для оператора обмена криптовалют.

Майнинг, деятельность оператора криптоплатформы, оператора обмена криптовалют, иная деятельность с использованием токенов не признаются банковской деятельностью;

LWO

ICO

4.4. юридическое лицо, создавшее и разместившее собственный токен через резидента Парка высоких технологий, обязано удовлетворять требования владельца токена, обусловленные при его создании и размещении. Отказ от удовлетворения требований владельца токена со ссылкой на отсутствие основания обязательства либо на его недействительность не допускается;

Конференции, семинары, лекции, обучение

4.5. деятельность юридических, физических лиц по организации и (или) проведению конференций, семинаров, лекций, обучающих и иных аналогичных мероприятий по вопросам создания и (или) использования технологии реестра блоков транзакций (блокчейн), иных технологий, основанных на принципах распределенности и безопасности совершаемых с их использованием операций, токенов осуществляется по согласованию с государственным учреждением ”Администрация Парка высоких технологий“;

LWO

Отличительные признаки блокчейн:

1. **Функционально: движение цифровых активов от лица к лицу (не хранилище данных или их контрольных характеристик)**
2. **Цепочка блоков**
3. **Транзакции**
4. **В подписываемой части поля: данные, открытый ключ получателя**
5. **Защищенность от «двойной траты» (применение закрепления блоков)**
6. **Доверенный способ хранения цепочки: какая цепочка истинная?**

Для чего нужна платформа:

для эмиссии и управления токенами (цифровыми активами).

Прикладные задачи:

- электронные деньги;
- контроль за движением товаров, услуг, прав;
- голосование;
- доверенной третьей стороны;
- иные системы, которые требуют гарантированной фиксации истории перемещения токенов.

LWO

Смарт-контракты

Над платформой работает система смарт-контрактов с обеспечением юридической значимости

LWO

Защита информации в блокчейн платформах

Обеспечение защиты информации: классика (без нее никуда, потому что нарушителей и угрозы никто не отменял), один из элементов защиты информации – технология блокчейн:

- цепочки транзакций (в транзакцию включается открытый ключ получателя и история);
- если выявляется угроза двойного расходования, то закрепление блоков транзакций;
- если выявляется угроза подмены данных, то несколько хранилищ данных со способом принятия решения о выявлении достоверных данных.

LWO

Защита информации в блокчейн платформах

???:

- Peer-to-peer;
- Proof of Work;
- применение национальных сертифицированных СКЗИ (как опция);
- постквантовая криптография;
- безопасность кошельков

LWO

Типы кошельков:

1. Облачные
2. Локальные
3. Аппаратные

LWO

БЛОКЧЕЙН ПЛАТФОРМА

Создание на базе платформ Bitcoin, Ethereum, … ?

1)надежность не прогнозируема;

2)доверие 50/50;

3)не постоянство (форки);

4)сложности разбора спорных ситуаций (правовой вакуум).

Вывод: не целесообразно. Быть может, для в случая наличия участников ИС, доверяющих этим платформам

LWO

Характеристика (требование)	**Принципиальное решение**
Уровень данных	Цепочка блоков
Управление данными	(P2P с ограниченным числом узлов)/(Распределенная/централизованная СУБД)
Закрепление блоков (с высокой централизацией)	~~PoW и аналоги~~ Аппаратные модули безопасности (HSM black boxes)
Криптозащита	CryptoAPI Использование как отечественных средств ЭЦП, так и из ядра ОС Применение постквантовых криптоалгоритмов – через CryptoAPI
Транзакция	Поддержка электронного документа (сертифицированное средство ЭЦП)
Токен	Универсальный/несколько цепочек
Носители ключей (кошельки)	Разные уровни безопасности. Разные способы депонирования и восстановления.
Аутентификация	Поддержка ГосСУОК, ЕС ИФЮЛ
Анонимность	Допускается в определенных случаях
Получение информации из платформы	В соответствии с правами доступа
Подключение прикладных информационных систем (Электронные деньги, Движение товаров, прав, …)	Через API
Архивирование	Возможность переопределения начала цепочки для уменьшения объема актуальной и архивного хранения не используемой части
Система защиты информации	Аттестована
Масштабируемость	+
Надежность	+
Высокое быстродействие	+
Эксплуатирующая организация	Выбор большой, начиная с Расчетного центра Национального банка

LWO

В ритме инноваций

lwo.by
contact@lwo.by

+375 17 334 10 02
+375 17 334 28 27

ул. Кропоткина, д. 91, Минск
Республика Беларусь, 220002