СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ ТЕХНОЛОГИИ БЛОКЧЕЙН

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

LWO

Развитие

- Отсеять худшее

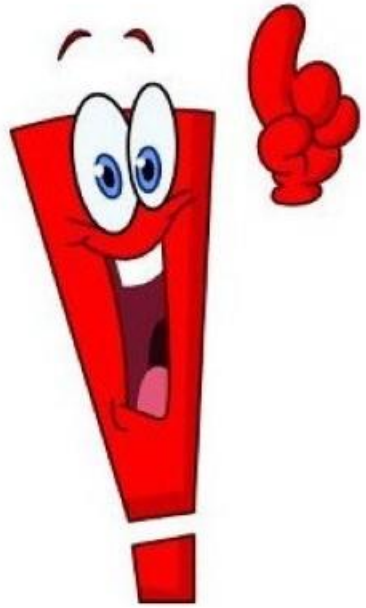
- Развивать лучшее

Составляющие технологии:

- В основе криптографические методы: электронная подпись, шифрование, хэширование, PKI, …
- Цепочки транзакций
- Закрепление блоков
- Пиринговая сеть для хранения данных
- Анонимность
- Право

Криптографические методы

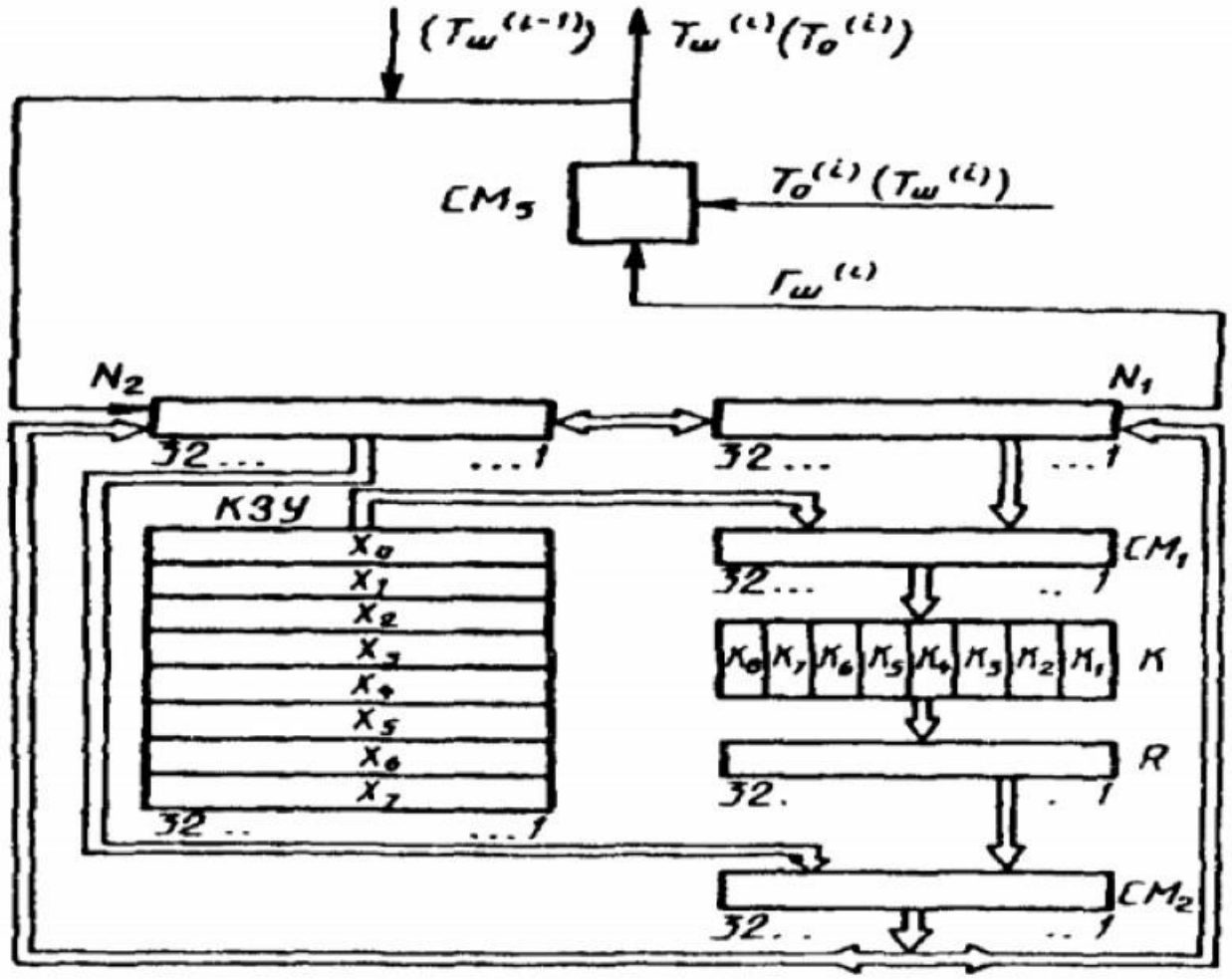
- Профильные конференции
- Безопасность блокчейн в постквантовом мире
- Использование постквантовых криптоалгоритмов



Цепочки транзакций

Гаммированние с обратной связью

С. 12 ГОСТ 28147—89



Черт 4

Цепочки транзакций

Цепочки транзакций

- (Я, Алиса, передаю цифровой актив Бобу) || подпись Алисы
  - Кто Алиса? Кто Боб? – связь с системой идентификации
- (Я, тот кто это подписал, передаю цифровой актив владельцу указанного ОК (ЛК)) || подпись
  - Более глубокие зависимости, анонимность
  - Авторизация – через PKI
- Связь между материальными сущностями и их электронно-цифровым представлением … была и будет оставаться проблемой ?
- Правовая база ?

Закрепление блоков транзакций

- Имеется возможность передачи одного цифрового актива нескольким получателям (двойная трата)
- Идея всеобщего майнинга не сработала
- Какая цепочка транзакций истинная?

Способ закрепления блоков транзакций

- Proof-of-Work

- Доверенными узлами

Пиринговая сеть

- Были и раньше. Используются и сейчас (тор, торренты)
- Проблема: рост объема БД
- Репликация, синхронизация

Скорость

- Наличные (материальные ценности) – теоретически не дублируются
- Цифровые активы – легко – двойная трата
- Необходимо ждать полной фиксации в системе
- Даже если все ПО работает моментально, то в совокупности это не меньше десятков секунд
- В существующих платежных системах (в ряде случаев) – моментально
- Диалектика: быстро передать – легко украсть!
- Криптобезопасность

Анонимность, конфиденциальность

- Введение авторизации (возможно частично)
- Обеспечение конфиденциальности … ?

Безопасное хранение ключей подписи

- Отличие от обычной подписи
- Особая роль надежного хранения ключей
- Депонирование ключей

Контроль передачи цифрового актива

Цепочки транзакций и закрепление блоков

- Конфиденциальность
- Целостность
- Доступность
- Сохранность
- Подлинность
- Возможность контроля передачи …?

Характеристики блокчейн платформ нового поколения

1. Надежные криптографические алгоритмы
2. Авторизация (анонимность – опционально)
3. Доверенные узлы (хранение данных; быстрое и надежное закрепление блоков)
4. Наличие способов обеспечения конфиденциальности, разграничение доступа
5. Надежность хранения ключей
6. Депонирование ключей, восстановление
7. Прозрачность для контролирующих органов
8. Стандартизация, открытые интерфейсы
9. Правовая база

Криптоанализ. Постановка задачи

1. Математическая модель
2. Программная модель
3. Сложность

Криптоанализ. Математическая модель

Криптографическая задача по поиску **nonce** в общем случае выглядит так:

Требуется найти n такой, что $H(M, n) < d$, где H – функция хэширования, d – сложность, M – данные. Эту задачу можно переписать в другом виде: Дано:

$$\begin{cases} H(M_0, r_0) = g_0, \\ H(M_1, r_1) = g_1, \\ H(M_2, r_2) = g_2, \\ \ldots\ldots\ldots\ldots \\ H(M_i, r_i) = g_i, \\ \ldots\ldots\ldots\ldots \end{cases}$$

Криптоанализ. Математическая модель

Это все **nonce**, которые были найдены за всю историю, причём существует подмножество таких, что их сложность меньше $H(M_i, r_i) < d$. Требуется найти такие $i\,(0 < i \leq d-1)$ и n_i такие, что $H(M, n_i) = i$.

В случае Ethereum неоднократно выбирается случайный **nonce** $\mathbf{n}_{rand} \in \mathbb{B}_8$ и вычисляется функция PoW, возвращающая массив из 2-х элементов, до тех пор, пока

$$\mathtt{PoW}(H_{\not d}, H_{\mathrm{n}}, \mathbf{d})[1] \leq \frac{2^{256}}{H_d}.$$

Криптоанализ. Математическая модель

Эта задача может быть расписана следующим образом. Дано: $\mathtt{PoW}(H_{\not\text{r}i}, H_{\text{r}_i}, \mathbf{d})\lfloor 1 \rfloor = g_i$ — **nonce**, которые были найдены за всю историю $(i \leq 4\,370\,000)$, причём среди них есть подмножество таких, что $\mathtt{PoW}(H_{\not\text{r}i}, H_{\text{r}_i}, \mathbf{d})\lfloor 1 \rfloor < \dfrac{2^{256}}{H_d}$. Требуется найти такие $i\left(0 < i \leq \dfrac{2^{256}}{H_d} - 1\right)$ и n_i такие, что $\mathtt{PoW}(H_{\not\text{n}i}, H_{\text{n}_i}, \mathbf{d})\lfloor 1 \rfloor = i$. Здесь функция $\mathtt{PoW}$, являющаяся массивом из 2-х элементов, определяется следующим образом:

$$\mathtt{PoW}(H_{\not\text{n}}, H_{\text{n}}, \mathbf{d}) = \left\{ \mathbf{m}_{\text{c}}\left(\mathtt{KEC}\left(\mathtt{RLP}\left(L_H(H_{\not\text{n}})\right)\right), H_{\text{n}}, \mathbf{d}\right),\right.$$

$$\left.\mathtt{KEC}\left(\mathbf{s}_{\text{h}}\left(\mathtt{KEC}\left(\mathtt{RLP}\left(L_H(H_{\not\text{n}})\right)\right), H_{\text{n}}\right) + \mathbf{m}_{\text{c}}\left(\mathtt{KEC}\left(\mathtt{RLP}\left(L_H(H_{\not\text{n}})\right)\right), H_{\text{n}}, \mathbf{d}\right)\right)\right\} =$$

Белорусское чудо

SMARTPOOL.BY

RU EN

SMARTPOOL.BY майнинг платформа

Пул для майнеров, желающих увеличить свой доход легальным способом

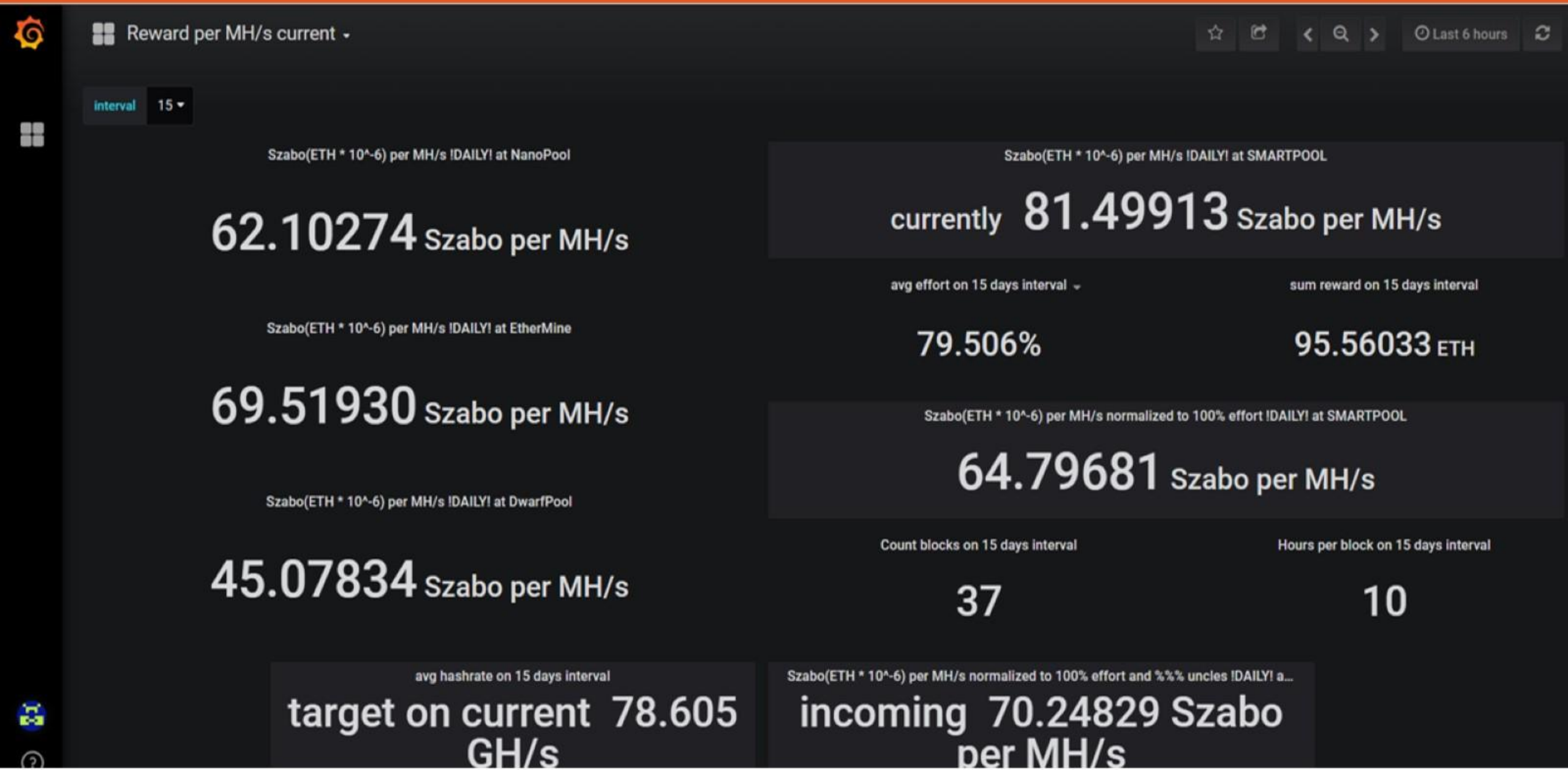
АЛГОРИТМ SMARTPOOL.BY
Обеспечиваем прозрачный и легальный майнинг ETH, ZEC, XMR
Узнать подробнее

МОНИТОРИНГ и SMARTBOARD
Обеспечиваем мониторинг майнинга и мониторинг состояния GPUs для каждого майнера с помощью SMARTBOARD
Узнать подробнее

ДОПОЛНИТЕЛЬНЫЕ ПЛЮСЫ
Обеспечиваем круглосуточные консультации, даем рекомендации, анонсируем ближайшие события
Узнать подробнее

Подключиться к пулу

Белорусское чудо: пул в числе лучших в мире



Спасибо тем,
кто верит и продвигает

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