



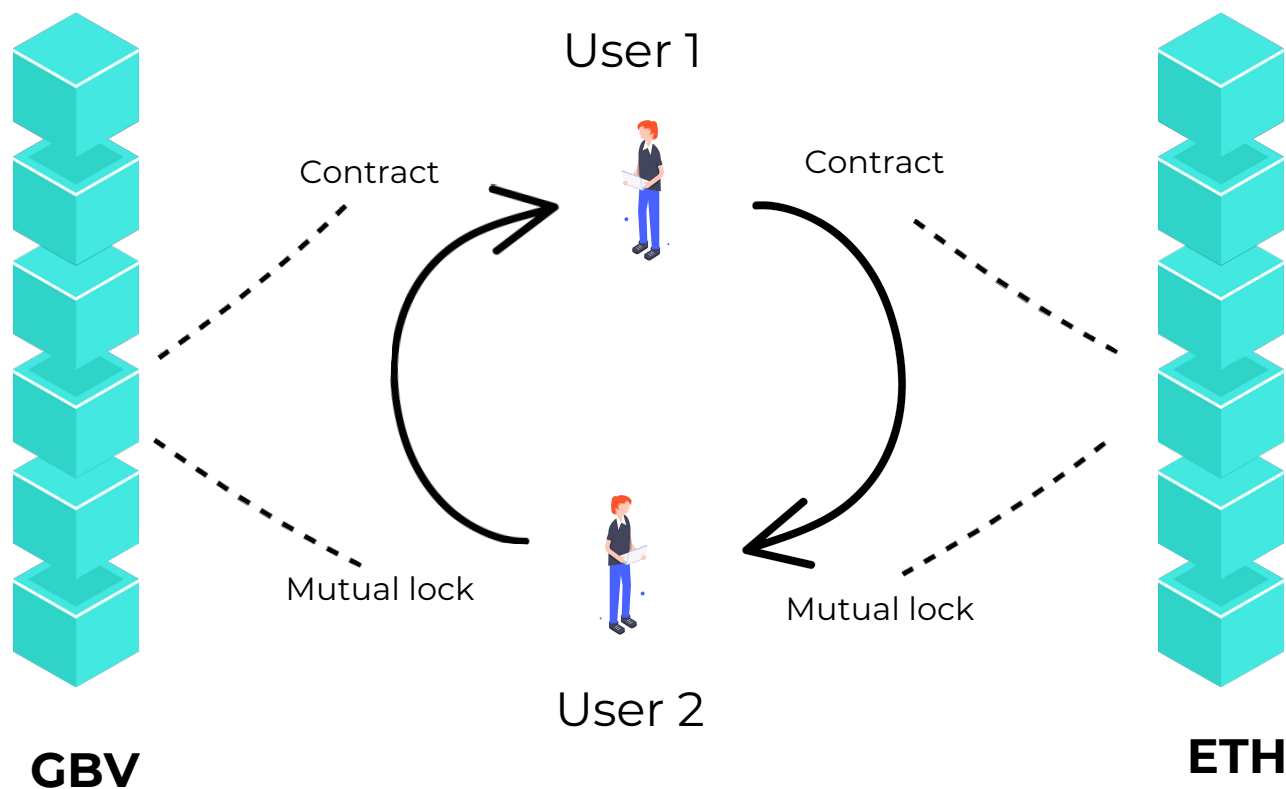
Атомарный своп (HTLC) [GBV - ETH]

Атомарные свопы - это метод функционирования цифровых активов, предоставляющий возможность быстрого обмена между двумя криптовалютами работающими на разных блокчейнах.

Этот процесс (также известный как атомарная кросс-цепная торговля) основан на смарт-контрактах и позволяет пользователям торговать монетами непосредственно со своего криптовалютного кошелька.



Принцип работы



Протоколы атомарных свопов разработаны таким образом, чтобы не допустить обмана со стороны любого из участников. Чтобы понять, как это работает, давайте представим, что User1 хочет обменять (GBV) на Эфир User2 (ETH).

Первым делом, User1 вносит депозит в ETH на адрес контракта, который выступает в качестве сейфа.

Когда этот сейф создан, User1 генерирует ключ для доступа к нему. Затем она делится криптографическим хэшем этого ключа с User2.



Затем User2 использует хеш, предоставленный User1 для создания другого безопасного адреса контракта на котором хранится его ETH. Чтобы получить ETH, User1 должен использоваться тот же ключ, таким образом предоставляя свою валюту User2 (благодаря специальной функции, которая называется хэшлок). Это означает, что как только User1 потребует ETH, User2 в свою очередь также запросит GBV, после чего обмен валютой будет завершен.

Термин «атомарный» относится к тому, что эти транзакции либо осуществляются в полном объеме или не происходят вовсе. Если одна из сторон не выполняет свои обязательства, то контракт аннулируется и средства автоматически возвращаются к их владельцам.

Атомарные свопы могут происходить двумя различными способами:

- в цепочке;
- вне цепочки.

Обратите внимание на то, что User2 пока что не может получить доступ к GBV, потому что у него есть только хэш ключа, а не сам ключ.



Что такое HTLC (Hash Timelock Contracts)

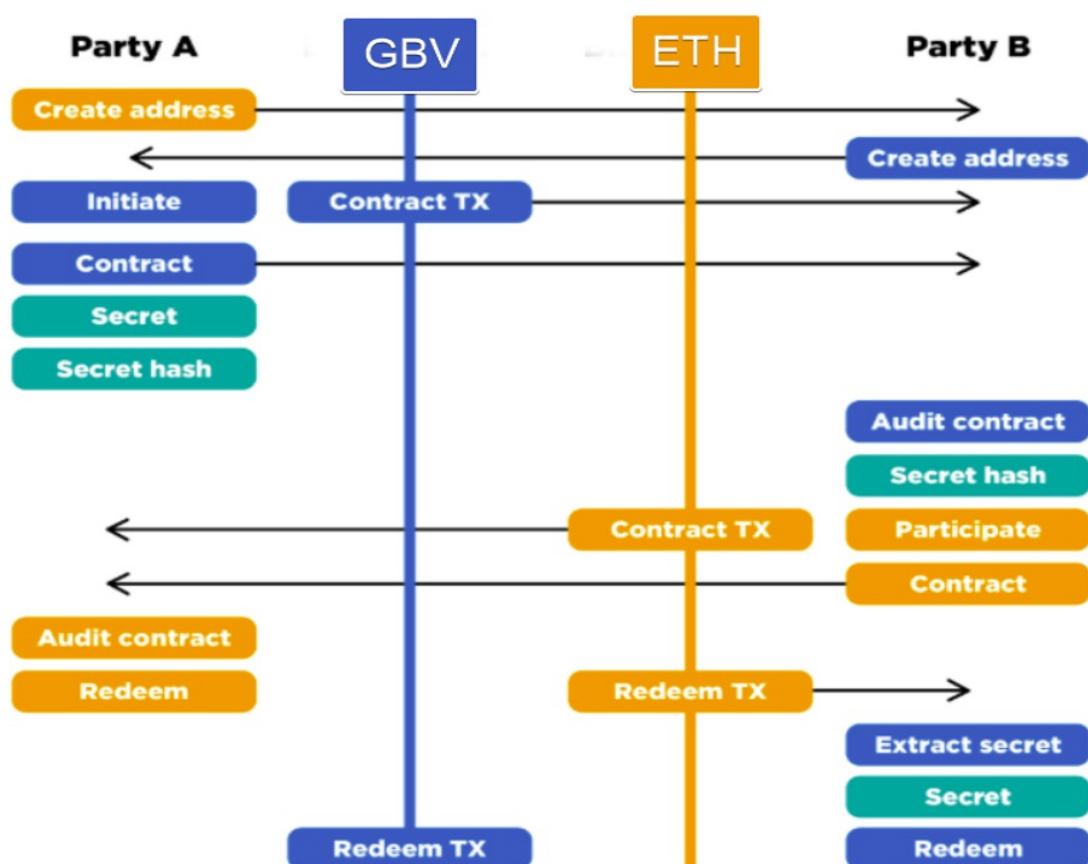
Hashed Timelock Contract (HTLC) – это тип интеллектуального контракта, используемого в каналах криптовалюты для устранения риска контрагента. Это позволяет осуществлять транзакции с привязкой по времени.

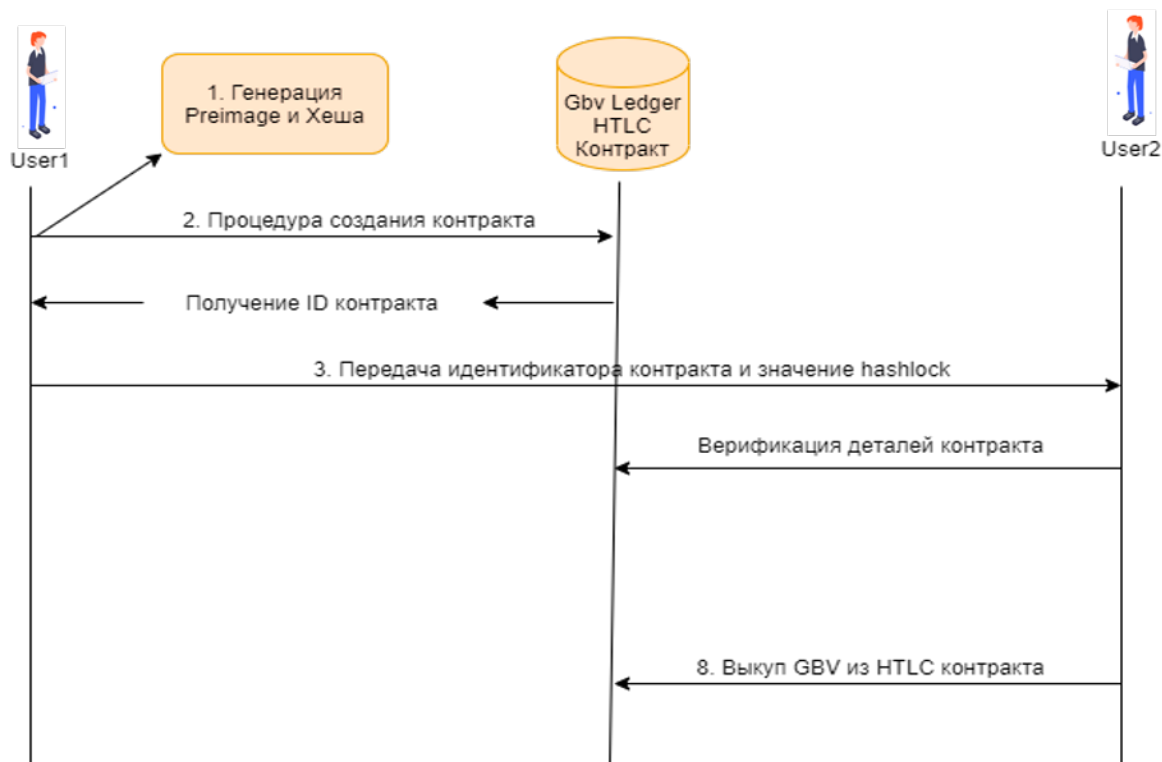
В практическом плане это означает, что получатели транзакции должны подтвердить платеж, создав криптографическое подтверждение в течение определенного периода времени. В противном случае транзакция не состоится.

В договоре хэшированной временной блокировки (HTLC) используются несколько элементов из существующих транзакций криптовалюты. Например, транзакции HTLC используют несколько подписей, которые состоят из частного открытого ключа, для проверки и проверки транзакций. Но есть два элемента, которые отличают HTLC от стандартных транзакций криптовалюты.

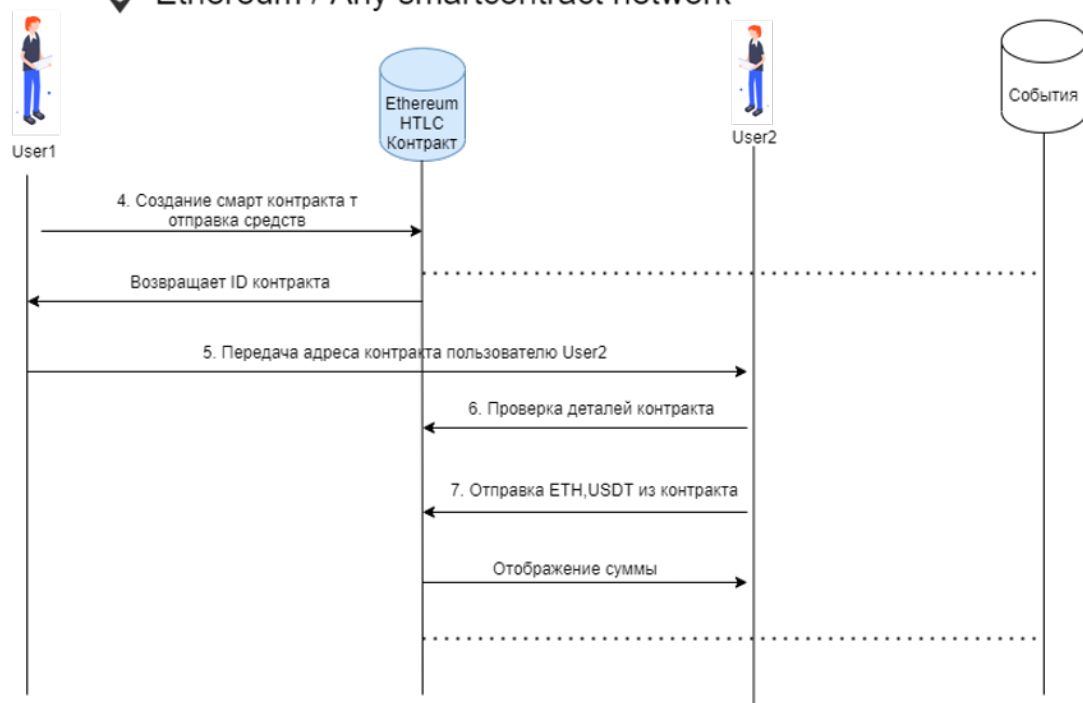


Схема взаимодействия между блокчейном GBV с блокчейном Ethereum.





◆ Ethereum / Any smartcontract network





Алгоритм работы

1. User1 выбирает случайное значение, которое мы назовём “preimage” и пропускает его через необратимую хеш-функцию, получая хешированное значение, которое мы назовём H.
2. Создается контракт между пользователем User1 и User2 в блокчейне GBV
3. Передача адреса контракта сгенерированному на шаге 2 к пользователю User2.
4. User2 Создает договор в сети Ethereum имея предоставленный preimage из шага 3. И передает средства на смарт контракт (резервирование).
5. Полученный идентификатор контракта из сети Ethereum передается пользователю User1.
6. User1 в сети Ethereum проверяет детали контракта
7. Отправка средств в сети Ethereum с контракта на кошелек User1