|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| *Шпаргалка*  *Версия от*  *20201206* | | | **Основные-** | | **Под-** (i ≥ 1) | |
| **Приватные** | **Публичные** | **Публичные** | **Приватные** |
| **ВНЕ БЛОКЧЕЙНА** (данные получателя платежа) | **Ключи траты** | | **Общий способ выведения ключей**    “ограниченная”  256-битная мнемоническая  фраза  **Мнемоническая** фраза из  24 + 1 (контрольная сумма)  слов, среди 1626  (162624 ≳ 2256)  **⋅ G**  s0    Hs | **S0 =** s0 **G** | **⋅ G**  **Si = Hs**(**“SubAddr”**|v0|**i** ) **G + S0**  **⋅ v0** | s**i = Hs**(**“SubAddr”** |v0|**i** ) **+** s0  **Фактически никогда не использовались:** подадреса были введены для общего использования v0 (для эффективности сканирования блокчейна)  **⋅ v0** |
| **Ключи**  **просмотра** | | **⋅ G**  v0 | **V0 =** v0 **G** | **⋅ G**  **Vi =** v0 **Si** | vi **=** v0 si |
| **Адреса** | | **Base58**( **0x12** | **S0** | **V0** | **checksum** ) **= “ 4 ……….” [95 знаков]**  **4-байтный урезанный хеш Keccak256** | | **Base58**( **0x2A** | **Si** | **Vi** | **checksum** ) **= “ 8 ……….” [95 знаков]**  **4-байтный урезанный хеш Keccak256** | |
| **Интегриро-ванные**  **адреса** | | **8-байтный компактный ID платежа, зашифрованный в платёжной транзакции (в сравнении с 32-байтным, который использовался ранее)**  **Base58**( **0x13** | **S0** | **V0** | **payID** | **checksum** ) **= “ 4 ……….” [106 знаков]**  **4-байтный урезанный хеш Keccak256** | | **Не используются, поскольку интегрированные адреса и подадреса некоторым образом решают ту же проблему**  Взято из <https://monerodocs.org/public-address/integrated-address/> :  “ […] для приёма платежей **отдельным пользователям** лучше использовать **подадреса**. В некоторых ситуациях это повышает уровень анонимности. Подробности содержатся в статье, посвящённой подадресам. **Предприятиям**, принимающим платежи автоматически, лучше использовать **интегрированные адреса**. Это объясняется следующим образом: […] ” | |
| **В БЛОКЧЕЙНЕ** (по инициативе плательщика) | **Ключи**  **транзакции** | | **⋅ G**  r | **R =** r **G** | **⋅ Si**  **R =** r **Si** | r |
| **Скрытые адреса** (t ≥ 0) | **POV**  **отправителя** | **Приватный ключ нельзя вывести на основе POV отправителя**, так как адрес является адресом назначения транзакции, получателя, которому переводятся средства отправителя | **Xt = Hs**( r **V0**|**t**) **G + S0**  Равенства остаются действительными благодаря связности r, R, v0, V0, Vi обеспечиваемой протоколом Диффи-Хеллмана  r (v0 **G**)  ⫴ | **Xt = Hs**( r **Vi**|**t** ) **G + Si**  r (v0 **Si**)  ⫴ | **Приватный ключ нельзя вывести на основе POV отправителя**, так как адрес является адресом назначения транзакции, получателя, которому переводятся средства отправителя |
| **POV**  **получателя** | **Используется для создания кольцевых подписей**, когда получатель становится отправителем и тратит свой UTXO  **⋅ G**  xt **= Hs**( v0 **R**|**t** ) **+** s0 | v0 (r **G**)  **Xt = Hs**( v0 **R**|**t** ) **G + S0** | v0 (r **Si**)  **⋅ G**  **Xt = Hs**( v0 **R**|**t** ) **G + Si** | **Используется для создания кольцевых подписей**, когда становится отправителем и тратит свой UTXO  xt **= Hs**( v0 **R**|**t** ) **+** si |
| **“Эллиптические примечания” J** | | | **Строчными** буквами обозначены **скалярные** величины, которыми также являются ивыходы Hs. **ЗАГЛАВНЫМИ** буквами обозначены **точки** на эллиптической кривой, используемой Monero (скрученная кривая Эдвардса Ed25519), даже если они могут быть представлены одним 256-битным значением благодаря технологии, известной как сжатие (в случае с адресами в полях протокола применялось представление, используемое при хешировании в соответствии с правилами арифметики на эллиптических кривых). Таким образом, при использовании точек эллиптической кривой, произведения и суммы должны восприниматься как их вариант на эллиптической кривой (при совершении действия в дискретном 2D пространстве), а не как обычные скалярные величины при работе со «значениями сжатых точек». **Hs( ) = sc\_reduce32( Keccak256( ) )** : выход хеша Keccak ограничивается **sc\_reduce32( )** из-за цикличности природы точек эллиптической кривой (отдельное спасибо Koe за соответствующее замечание); следует отметить, что то же ограничение применяется к приватному ключу транзакции **r** и к указанному **методу выведения ключа мнемонической фразы, состоящей из 25 слов** (равно как и к любому другому). | | | |
| **Примечания**  **и ссылки** | | | [**Изучаем Monero**](https://masteringmonero.com/free-download.html) **[**[**RU**](https://github.com/monerobook/monerobook/tree/master/translations/ru)**]** (первая редакция - декабрь 2018 / бесплатная PDF версия - 18 апреля 2019 - SerHack и Сообщество Monero) **ПРИМЕЧАНИЕ:** форма этой шпаргалки немного отличается  [**От нуля к Monero: Вторая**](https://www.getmonero.org/library/Zero-to-Monero-2-0-0.pdf) **редакция [**[**RU**](https://github.com/UkoeHB/Monero-RCT-report/tree/master/translations/ru)**]** (v2.0.0 - 4 апреля2020 - Koe, Курт М. Алонсо, Саранг Нёзер) главы 1, 2, 4 от исходного варианта в целях обеспечения  [**Обзор белой книги Cryptonote**](https://www.getmonero.org/resources/research-lab/pubs/whitepaper_review.pdf)(июль 2014 ? - Брэндон Гуделл AKA Шурэ Нёзер) “понимания с первого взгляда”  [[**Как создаются адреса**](https://xmr.llcoins.net/addresstests.html) **в Cryptonote**](https://xmr.llcoins.net/addresstests.html) (luigi1111)  Различные темы на [**Monero Stack Exchange**](https://monero.stackexchange.com/) и [**Monerodocs**](https://monerodocs.org/) | | | |