Bitcoin Post-Quantum

Noah Anhao
noahanhao@bitcoinpq.org

1. Введение

Безопасность децентрализованной цифровой валюты Биткойн основывается на алгоритме цифровой подписи в группе точек эллиптической кривой (ECDSA), который позволяет произвести авторизацию плательщика, и алгоритме доказательства выполненной работы (Proof of Work), который не позволяет плательщику расплатиться одними и теми же деньгами более одного раза.

Биткойны перемещаются к новому владельцу посредством транзакции с адреса на адрес, адрес является хешем от публичного ключа получателя или скрипта. Публичный ключ отправителя раскрывается в момент распространения транзакции по сети. Владение биткойнами равносильно владению секретным ключом от соответствующего адреса, а доказательством права владения является цифровая подпись, которой подписывается транзакция.

Криптостойкость ECDSA основывается на сложности задачи дискретного логарифмирования в группе точек эллиптической кривой (ECDLP), которая решается за экспоненциальное время, то есть является сложной для классического компьютера. Квантовый алгоритм Шора для вычисления дискретных логарифмов в конечных полях позволяет вычислить секретный ключ ECDSA по публичному ключу за полиномиальное время, то есть существенно проще. Это ставит под угрозу как ранее использованные для траты адреса с ненулевым балансом, так и еще не включенные в блок транзакции. При распространении транзакции по сети происходит раскрытие публичного ключа, и у атакующего есть время до включения этой транзакции в следующий блок для вычисления секретного ключа с помощью квантового компьютера и создания поддельной транзакции с верифицируемой цифровой подписью.

К счастью, есть задачи, пригодные для использования в схемах цифровой подписи и при этом в достаточной мере сложные как для классического, так и для квантового компьютера. К таким задачам относится нахождение прообраза хеша. Квантовый алгоритм Гровера для поиска по несортированным базам данных позволяет решить задачу восстановления хеша за время порядка квадратного корня из классического, что является огромным ускорением, но сложность задачи по прежнему остается экспоненциальной, поэтому необходимый уровень криптостойкости достигается использованием хеш-функции соответствующей длины. Это позволяет считать криптографические системы, основанные на хешировании, квантово-безопасными. Согласно рекомендациям PQCRYPTO (Европейский консорциум университетов и компаний, занимающийся вопросами постквантовой криптографии), в

качестве квантово-устойчивой цифровой подписи следует использовать расширенную схему подписи Меркла (XMSS), она сочетает в себе высокий уровень безопасности, приемлемое время генерации ключа и размер подписи по сравнению с другими предложенными научным сообществом постквантовыми алгоритмами электронной подписи.

Bitcoin Post-Quantum (BPQ) является экспериментальным ответвлением основного блокчейна Биткойна с квантово-безопасными цифровыми подписями. В дальнейшем опыт BPQ может пригодится для внедрения квантово-безопасной криптографии в основную ветку Биткойна. Также Bitcoin Post-Quantum удовлетворяет актуальную потребность в резервном блокчейне на случай внезапного скачка в развитии технологий, которые способны поставить под угрозу безопасность популярных криптовалют.

Невозможно точно предсказать, когда квантовые компьютеры станут достаточно мощными, чтобы взломать популярные криптографические схемы, известно только то, что это произойдет в обозримом будущем.

Несколько фактов, свидетельствующих о своевременности нашей разработки:

- в 2015 году Агентство Национальной Безопасности США (NSA) объявило о планах по переходу на постквантовые криптографические алгоритмы: “К сожалению, рост использования эллиптической кривой столкнулся с фактом продолжающегося прогресса в исследованиях в области квантовых вычислений, который дал понять, что криптография на эллиптических кривых не является долговременным решением, как считалось ранее.” [1];

- в 2016 году IBM предоставил [2] первый облачный квантовый компьютер IBM Q на 5 кубит для всех желающих попрактиковаться в квантовом программировании;

- в 2016 инженеры Intel объявили [3] о работе над квантовым процессором на миллионы кубит;

- в 2016 году разработчики Google Chrome внедрили [4] постквантовый алгоритм обмена ключами New Hope, а в 2017 году в Google спрогнозировали [5] коммерциализацию квантовых технологий в ближайшие 5 лет;

- в апреле 2018 в обновлении OpenSSH 7.7 разработчики внедрили [6] постквантовый алгоритм цифровой подписи XMSS;

- в июне 2018 Microsoft добавил [7] постквантовые алгоритмы обмена ключами и подписи в форк OpenVPN.

2. Квантовые Вычисления

На глубоком уровне реальности каждая элементарная частица вещества является не просто точкой в пространстве состояний, а представляется “облаком” своих возможных состояний. Например, одиночный фотон, проходящий через экран с двумя прорезями шириной около его собственной длины волны, проходит сразу через обе прорези, после чего разные варианты фотона, движущиеся по разным траекториям, взаимодействуют между собой, о чем свидетельствует интерференционная картина на проекционном экране, возникающая при многократном повторении опыта [8]. Говорят, что частица находится в *суперпозиции* своих возможных состояний.

На пространстве состояний задается функция, которая полностью описывает квантовый объект, она называется волновой функцией. Инструментальный смысл волновой функции состоит в том, что квадрат ее модуля равен вероятности обнаружения частицы в определенном состоянии после измерения. Измерение состояния квантового объекта приводит к расщеплению возможных путей эволюции квантовой системы как отдельных потоков реальности, в которых конкретизируется измеряемая величина, состояние прибора и самого наблюдателя, поэтому измерение всегда дает конкретное значение с некоторой вероятностью.

Так как состояние можно измерить, то можно выбрать подходящий квантовый объект и его характеристику для измерения, договориться о кодировании битов 0 и 1 и использовать квантовое состояние как носитель информации. Квантовый объект можно предсказуемым образом ввести в состояние суперпозиции, которое одновременно кодирует 0 в одной части вариантов реальности и 1 — в другой. Так возникает абстрактное математическое понятие кубита (q-bit, квантовый бит) без привязки к конкретной физической реализации. Алгоритмы, исполняемые на квантовых компьютерах, представляют собой последовательные преобразования состояний кубитов. Алгебраически это выглядит как умножение унитарных матриц квантовых вентилей на векторы состояний кубитов. Таким образом во всех вариантах реальности происходит своя часть полезных вычислений со своими входными данными, а комбинирование промежуточных результатов вычислений осуществляется посредством интерференции, как показано на Рисунке 1. Последней операцией квантового алгоритма обычно является измерение состояний кубитов.

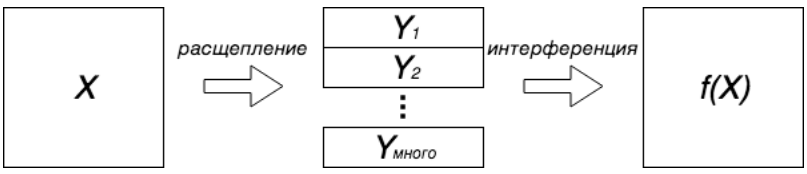

Рисунок 1. Типичное квантовое вычисление. Y_1 … $Y_{много}$ — промежуточные результаты, зависящие от входа *X*. Все они необходимы для эффективного вычисления выхода *f(X)* [9]

Как показал Deutsch [10], универсальный квантовый компьютер может имитировать различные физические системы, реальные и теоретические, которые выходят за рамки универсальной машины Тьюринга. Это позволяет существенно упростить решение некоторых видов задач, которые доказано невозможно быстро решить в рамках классических вычислений, в частности это относится к задачам криптологии.

В 1994 году Shor [11] предложил квантовые алгоритмы дискретного логарифмирования в группе точек эллиптической кривой и факторизации чисел. В 2001 году в IBM [12] продемонстрировали работоспособность алгоритма Шора, разложив число 15 на множители 3 и 5 на 7-кубитном квантовом компьютере. По оценке Proos и Zalka [13] восстановление секретного ключа ECDSA длиной 256 бит потребует около 1500 кубит и $6*10^9$ ($\sim 2^{32}$) операций. По оценке специалистов Microsoft [14] для этого потребуется 2330 кубит и $1.26*10^{11}$ ($\sim 2^{36}$) операций.

Для подписывания транзакций в Биткойне используется эллиптическая кривая secp256k1, она обеспечивает 128-битную классическую криптостойкость. В скором будущем в Биткойне будет использоваться схема подписи Шнорра, которая также основывается на сложности дискретного логарифмирования и поэтому также не является квантово-безопасной.

Анализ блокчейна Биткойна показал [15], что по состоянию на июнь 2018 у около 19% адресов, на которых хранятся 36% биткойнов, публичные ключи находятся в открытом виде, поэтому эти средства подвержены квантовой атаке в первую очередь. Остальные биткойны находятся на одноразовых адресах, поэтому в меньшей мере подвержены атаке, так как их публичные ключи публикуются лишь в момент траты и у атакующего остается немного времени для попытки совершения двойной траты до момента включения транзакции в блок. До этого момента публичные ключи хранятся в хешированном виде под 160-битным хешем RIPEMD160(SHA2-256(pubkey)) для P2(W)PKH и P2SH адресов и под 256-битным хешем SHA2-256(pubkey) для P2WSH-адресов.

Квантовый алгоритм Гровера [16] для поиска по несортированным базам данных позволяет решить задачу восстановления хеша за время порядка квадратного корня из классического, что является огромным ускорением, но сложность задачи по прежнему остается экспоненциальной. Таким образом постквантовая криптостойкость 160-битной хеш-функции RIPEMD160 составляет 80 бит, поэтому биткойны на одноразовых адресах находятся в относительной безопасности по сравнению с биткойнами на адресах с раскрытыми публичными ключами. Чтобы получить нужную постквантовую криптостойкость (как минимум 128 бит), нужно выбрать хеш-функцию соответствующей длины. 256-битные хеши, используемые в P2WSH-адресах, обеспечивают достаточную 128-битную постквантовую криптостойкость, пока не раскрыты соответствующие им публичные ключи. Стоит отметить, что в новых P2WSH-адресах ввели 256-битную хеш-функцию вместо 160-битной с другой целью — чтобы обеспечить 128-битную устойчивость от коллизий для защиты от атаки дней рождений при использовании мультиподписей.

3. Постквантовая Криптография

Постквантовая криптосистема это такая система, что при атаке на неё квантовый компьютер не имеет преимуществ перед классическим. Известные алгоритмы постквантовой криптографии с открытым ключом основываются на различных подходах [17], которые включают в себя: хеш-функции, изогении суперсингулярных эллиптических кривых, коды исправления ошибок, решётки, многомерные квадратичные уравнения.

Криптостойкость цифровой подписи, основанной на хешировании, сводится к устойчивости хеш-функции к восстановлению первого и второго прообраза. Восстановление прообраза хеша длиной n бит на классическом компьютере сводится к полному перебору (сложность $O(2^n)$), на квантовом — к перебору алгоритмом Гровера (сложность $O(2^{n/2})$). Таким образом, можно выбрать стойкую хеш-функцию, обеспечивающую необходимую классическую и постквантовую криптостойкость. Другие подходы к постквантовой криптографии основываются на математических проблемах, которые считаются квантово-устойчивыми, но возможно могут быть решены классическим компьютером в случае прорыва в развитии математики.

Согласно рекомендациям PQCRYPTO [18] для достижения 128-битной постквантовой криптостойкости в Bitcoin Post-Quantum используется схема цифровой подписи XMSS [19] с параметрами из RFC 8391 [20]. Недостаток схемы XMSS состоит в том, что она может генерировать ограниченное число подписей, которое зависит от высоты используемого дерева Меркла.

Наряду с XMSS рекомендации PQCRYPTO включают в себя схему SPHINCS [21], которая лишена ограничения на количество подписей, но для 128-битной криптостойкости размер такой подписи составляет около 41 килобайт, что слишком дорого для использования в блокчейне и в большей степени пригодно для использования в системах аутентификации. Размер подписи XMSS составляет около 2.5 килобайт, что довольно много по сравнению с подписью ECDSA (71 байт) и требует увеличения размера блока, но является наиболее оптимальным вариантом для постквантовой подписи в блокчейне.

a. Одноразовая Подпись Винтерница (W-OTS+)

Важным криптографическим примитивом является одноразовая подпись (One-Time Signature, OTS), которая предполагает одноразовое использование ключа для подписывания сообщения. Подписание двух разных сообщений одним ключом небезопасно. В Bitcoin Post-Quantum используется вариант схемы одноразовой подписи Винтерница (W-OTS+), описанный Hülsing [22] и представленный на Рисунке 2.

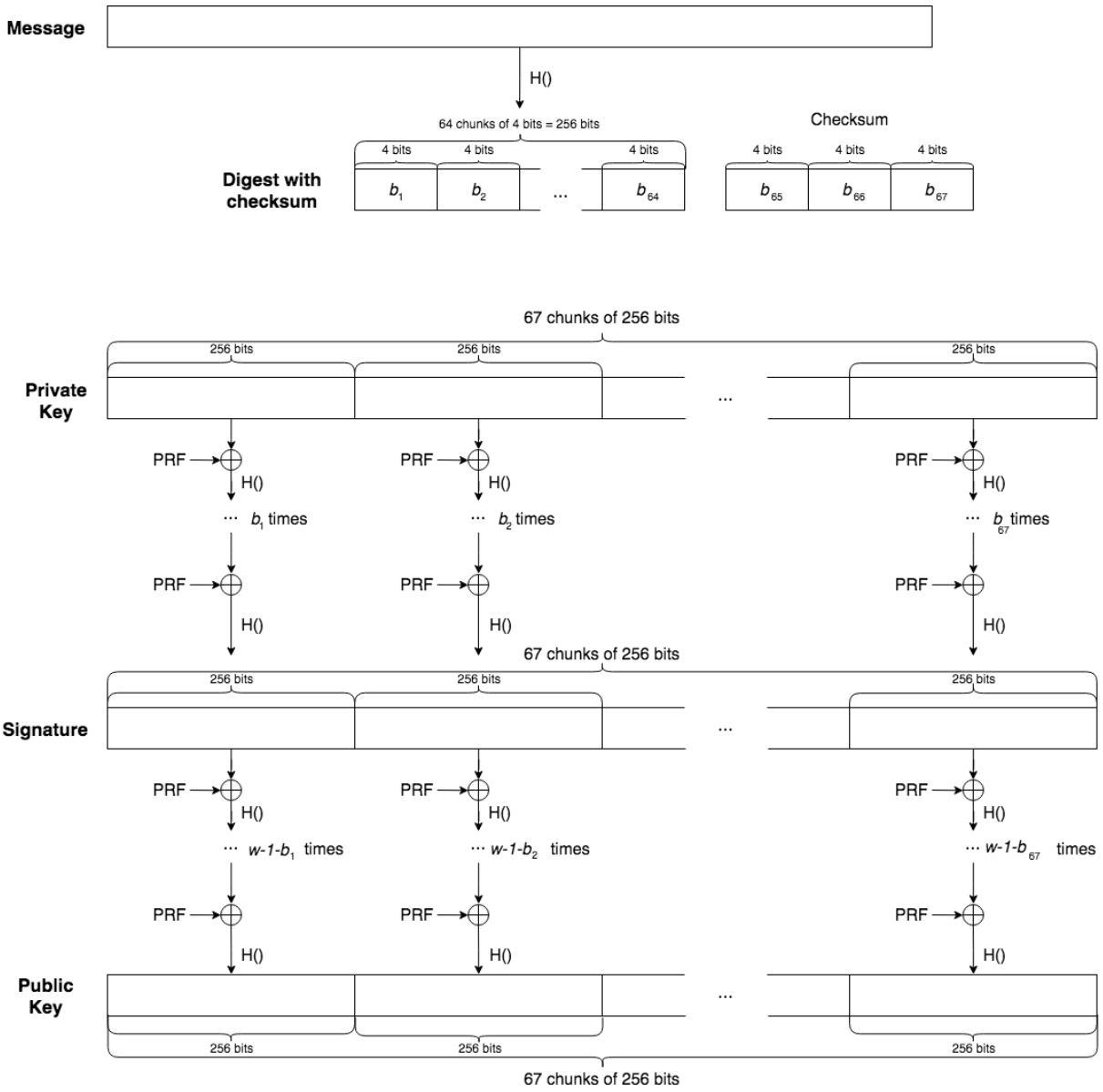

Рисунок 2. Схема W-OTS+ (n = 32, m = 256, w = 16)

Bitcoin Post-Quantum использует W-OTS+ с параметрами n = 32, m = 256, w = 16. n — параметр безопасности, который задает длину в байтах хеша используемого в итерациях алгоритма подписи, m задает битовую длину хеша подписываемого сообщения, w — параметр Винтерница, который определяет соотношение между используемой памятью и временем работы.

Секретный ключ представляет из себя набор случайно сгенерированных 256-битных чисел. Их количество ($l = l_1 + l_2$) определяется параметрами m и w:

$$\ell_1 = \left\lceil \frac{m}{\log(w)} \right\rceil, \quad \ell_2 = \left\lfloor \frac{\log(\ell_1(w-1))}{\log(w)} \right\rfloor + 1, \quad \ell = \ell_1 + \ell_2.$$

В нашем случае $l = l_1 + l_2 = 64 + 3 = 67$.

Для вычисления публичного ключа, каждое из этих 67 256-битных чисел XOR-ится с битовыми масками, возвращаемыми псевдо-случайной функцией (PRF) и хешируется $w - 1 = 15$ раз. В качестве хеш-функции и PRF используется SHAKE-128(256 бит). Битовые маски PRF генерируются на основе случайного seed-значения.

Для подписывания сообщения, вычисляется его 256-битный хеш и 12-битная контрольная сумма. Хеш сообщения с контрольной суммой (вместе 268 бит) делится на 67 4-битных чисел $b_1, b_2, \ldots, b_{67}$. Каждое из 67 чисел секретного ключа хешируется b_i раз, полученные 67 256-битных чисел составляют подпись.

Для верификации каждое из 67 чисел подписи хешируется $15 - b_i$ раз и сверяется с соответствующими значениями публичного ключа.

Контрольная сумма прибавляется к хешу подписываемого сообщения с целью недопущения раскрытия секретного ключа в том случае, если хеш сообщения будет состоять полностью из нулей.

b. Расширенная Схема Подписи Меркла

Расширенная схема подписи Меркла (XMSS, eXtended Merkle Signature Scheme) [19] позволяет собрать множество одноразовых публичных ключей W-OTS+ в один публичный ключ, таким образом XMSS дает возможность использовать один и тот же публичный ключ много раз.

Для построения дерева XMSS высоты h случайным образом генерируется seed-значение, из которого порождаются 2^h секретных ключей W-OTS+ и соответствующие им публичные ключи. Из каждого публичного ключа W-OTS+, который состоит из l чисел, строится бинарное L-дерево. Числа публичного ключа являются листками L-дерева. Так как l не обязательно является степенью двойки (как было показано выше, в нашем случае $l = 67$), то узел дерева, который не имеет справа пары, поднимается на уровень выше, пока не станет правой парой для другого узла, как показано на Рисунке 3.

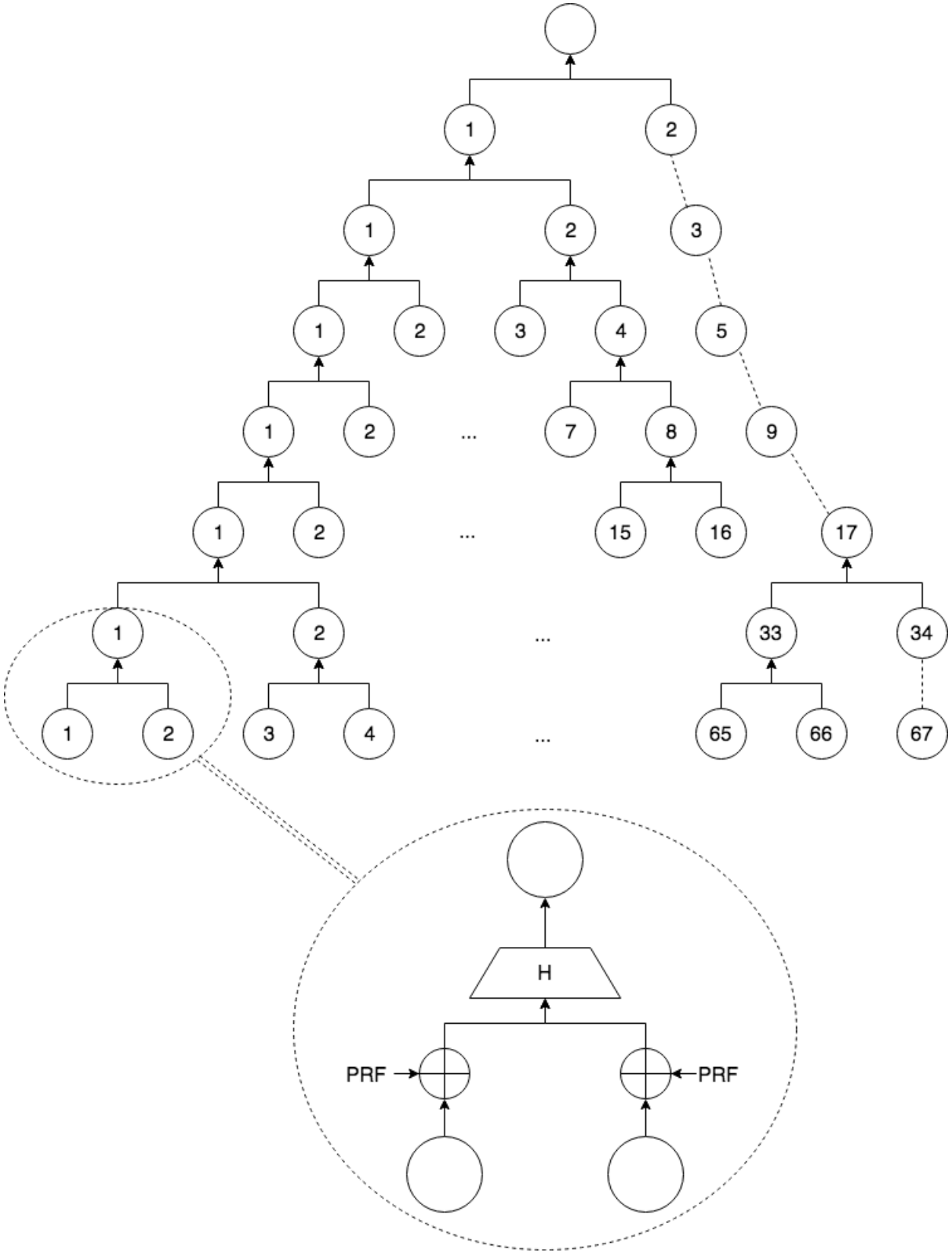

Рисунок 3. Схема построения L-дерева

Корень каждого из 2^h L-деревьев становится листком дерева Меркла, как показано на Рисунке 4. Корень дерева Меркла в свою очередь становится публичным ключом XMSS.

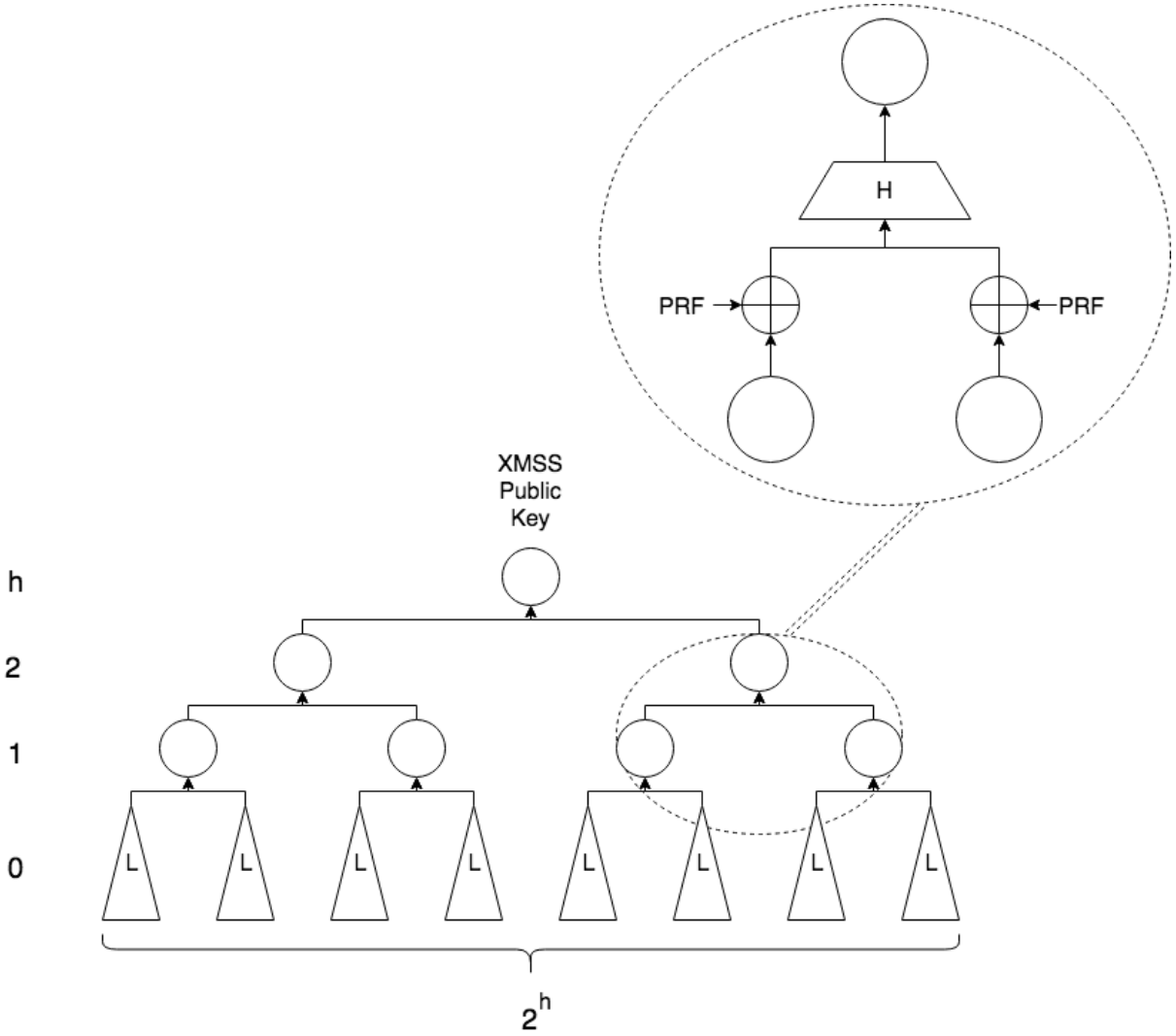

Рисунок 4. Схема построения дерева XMSS

При подписании транзакции используется первый неиспользованный ключ W-OTS+. Подпись XMSS содержит подпись W-OTS+ и путь аутентификации — последовательность узлов дерева, необходимых для вычисления корня дерева Меркла.

К примеру, пусть для подписания транзакции используется узел (0,5) как на Рисунке 5. Чтобы проверяющий мог вычислить узел (1,3), в путь аутентификации добавляется узел (0,6). Далее — для вычисления узла (2,2) нужен узел (1,4), аналогично для вычисления корня (3,1) понадобится узел (2,1). Таким образом, путь аутентификации будет содержать узлы (0,6), (1,4), (2,1) и вместе с подписью W-OTS+ это позволяет верифицировать подпись, рассчитав корень дерева Меркла и сверив его с публичным ключом XMSS.

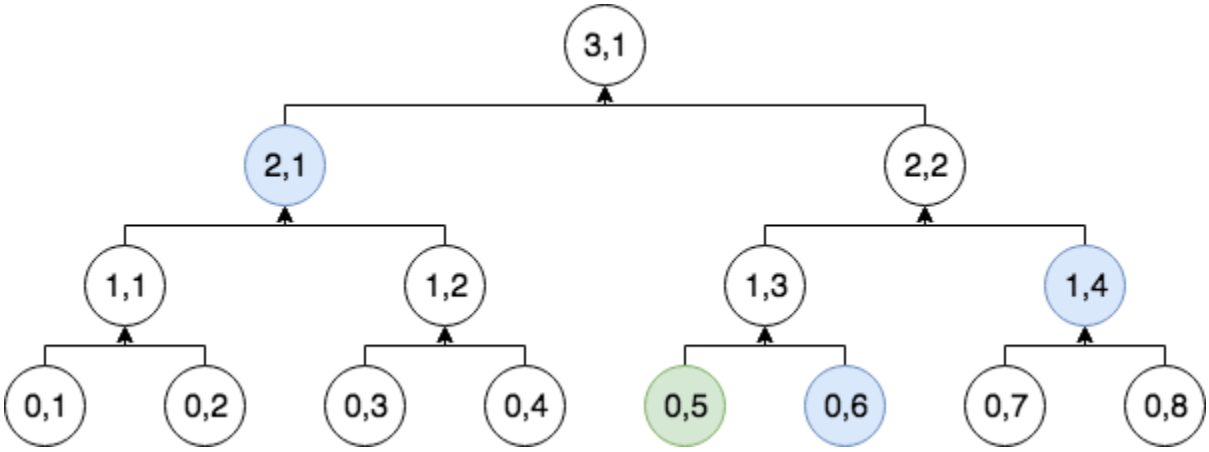

Рисунок 5. Путь аутентификации

Используя деревья XMSS разной высоты h, можно получить необходимое количество подписей. В BPQ используются параметры из RFC 8391 [20]:

Name	Function	n	w	len	h
XMSS-SHAKE_10_256	SHAKE128(256 bits)	32	16	67	10
XMSS-SHAKE_16_256	SHAKE128(256 bits)	32	16	67	16
XMSS-SHAKE_20_256	SHAKE128(256 bits)	32	16	67	20

Дерево XMSS высотой $h = 10$ позволяет подписать $2^{10} = 1024$ транзакций, высотой $h = 16$: $2^{16} = 65536$ транзакций, высотой $h = 20$: $2^{20} = 1048576$ транзакций. Чем больше дерево, тем дольше происходит его генерация. На современном компьютере создание дерева высотой $h = 10$ длится менее секунды, $h = 16$ - менее минуты, $h = 20$ около 10 минут.

4. Постквантовый Форк Биткойна

a. Хардфорк Блокчейна

В рамках существующего консенсуса в Биткойне принимаются только те транзакции, которые имеют действительную цифровую подпись ECDSA. Блоки, содержащие транзакции, подписанные XMSS, будут отвергаться Биткойн-нодами.

Консенсус в Bitcoin Post-Quantum действует следующим образом: до блока высотой 555,000 правила работы сети идентичны сети Биткойн, а начиная с этого блока будут действовать новые правила, в соответствии с которыми вводится

поддержка квантово-безопасных подписей XMSS, увеличивается размер блока и изменяется алгоритм майнинга.

Владельцы биткойнов на момент хардфорка автоматически получают такое же количество монет в блокчейне BPQ. Чтобы защитить свои монеты от взлома с применением квантового компьютера, они должны будут создать новые ключи для XMSS и сделать транзакцию со своих старых адресов на новые. Транзакции на адреса старого типа не поддерживаются стандартным программным обеспечением. Хотя такие транзакции могут быть созданы вручную и приняты сетью, но выходы таких транзакций не смогут быть потрачены с использованием ECDSA.

Примерно через год после запуска основной сети BPQ поддержка старых цифровых подписей на эллиптической кривой будет полностью отключена. Монеты, которые к тому времени не будут защищены от квантовой атаки путем перевода на квантово-безопасные адреса, будут сожжены. Таким образом, утерянные ранее ключи не будут скомпрометированы в блокчейне Bitcoin Post-Quantum. Награда за майнинг будет увеличена таким образом, чтобы финальная эмиссия монет оставалась равной 21,000,000.

Программный код Bitcoin Post-Quantum является форком Bitcoin Core 0.16.0 и включает в себя поддержку SegWit. Следовательно, в BPQ не стоит проблема пластичности транзакций и он готов для построения Lightning Network.

b. Квантово-Безопасные Адреса

В Bitcoin Post-Quantum используются модифицированные bech32-адреса следующего вида:

MAINNET: pq1p7mpu6tdds2q08dwvwn0srr886jej4suupqzkedn5sv48wgg5anmsprg42s

TESTNET: tq1peewnl23ptz9c0askjems7adpat6f7h9qa8l38h0th23lnyw7v0uqkthefn

REGTEST: pqrt1pnfn3yvfr4lenlpk09zmrcktw6eu0qt849cunxc0f8lnts8znv9sq0alx6w

По аналогии с P2WSH адресами Биткойна, квантово-безопасный адрес Bitcoin Post-Quantum состоит из удобочитаемой части “pq”, разделителя “1”, witness program (значение witness version установлено в “1”) в модифицированной кодировке base32 и контрольной суммы.

Адреса P2(W)PKH намеренно не используются. Деньги с квантово-безопасных адресов могут быть потрачены скриптами всех типов — как требующими одиночную подпись ([pubkey] OP_CHECKSIG), так и мульти-подпись (*m* [pubkey$_1$] … [pubkey$_n$] *n* OP_CHECKMULTISIG), так и любыми другими. Общий внешний вид адреса для всех типов скриптов дает дополнительное преимущество в виде обфускации функционального назначения адреса.

Чтобы получить баланс в блокчейне Bitcoin Post-Quantum пользователи, владеющие монетами в основном блокчейне Биткойна на момент форка, должны будут сгенерировать ключ XMSS и соответствующий ему pq-адрес, ввести в программу-кошелек свои старые ECDSA ключи и совершить первую транзакцию на новый адрес со своих старых адресов. Транзакции со старых адресов на старые адреса не поддерживаются.

Внимание! В целях безопасности перед тем, как вводить старые ECDSA ключи в программу-кошелек, настоятельно рекомендуется перевести с них деньги в основном блокчейне Биткойна на адреса, управляемые другими ключами.

c. Размер и Вес Блока

Все транзакции Bitcoin Post-Quantum являются SegWit-транзакциями (за исключением транзакций со старых legacy-адресов Биткойна). Квантово-безопасные подписи имеют большой размер в сравнении с ECDSA-подписями, поэтому соотношение масштабирования (WITNESS_SCALE_FACTOR) увеличено с 1:4 до 1:32 так, чтобы пропускная способность сети оставалась такой же, как в Биткойне при текущих средних количестве и конфигурациях транзакций. Таким образом, максимальный вес блока увеличен с 4 миллионов до 32 миллионов единиц веса за счет увеличения witness-части блока, в то время как ограничение размера обычной части блока остается равным 1 мегабайт. Это приводит к фактическому размеру полностью заполненного блока около 16 мегабайт.

d. Алгоритм Консенсуса

Алгоритм выполненной работы (Proof of Work, PoW) в Биткойне состоит в переборе случайного значения специального поля (nonce) заголовка блока до тех пор, пока двойной SHA2-256 хеш заголовка блока не окажется меньше некоторого целевого числа (target), которое автоматически рассчитывается каждые 2,016 блоков на основании предыдущего значения и временных меток блоков так, чтобы дальнейший перебор при текущей скорости перебора хешей длился около 10 минут.

Атака на PoW Биткойна состоит в том, чтобы завладеть большей частью вычислительных мощностей сети. Это позволило бы атакующему произвести двойную трату — то есть потратить свои деньги в текущей цепи блоков, а параллельно рассчитать и немного позже опубликовать альтернативную цепочку достаточной длины, в которой отправить свои деньги на другой адрес. Согласно правилам консенсуса, участники сети признают верной более длинную цепь блоков.

Квантовый алгоритм Гровера обеспечивает квадратичное ускорение по сравнению с классическим поиском подходящего значения nonce для задачи подбора блока, что делает перспективным производство квантовых устройств для майнинга.

Это в свою очередь ведет к централизации вычислительных мощностей и повышает шансы успешной атаки 51% [23] в еще большей степени, чем есть на сегодняшний день.

Как показал Bernstein [24], квантовый компьютер экономически гораздо менее эффективен, чем классический для параллельного поиска коллизий хеш-функций. Например, для сокращения времени работы квантового алгоритма с $O(2^{n/2})$ до $O(2^{n/3})$ потребуется $O(2^{n/3})$ независимых модулей, а для такого же ускорения классическому компьютеру понадобится всего $O(2^{n/6})$ модулей. Таким образом, квантовые вычислительные устройства не помогут в задаче поиска коллизий, в отличие от задачи подбора прообраза, для которой они обеспечивают квадратичное ускорение.

Алгоритм PoW Equihash [25], используемый в криптовалюте Zcash, основывается на обобщенной задаче дней рождений. Задача *Equihash*(n, k, d) состоит в нахождении 2^k чисел $(i_1, i_2, \ldots, i_{2^k})$ длиной $(n/(k+1))+1$ бит таких, что выполняются два условия (H() – хеш-функция Blake2b):

$$H(i_1) \oplus H(i_2) \oplus \ldots \oplus H(i_{2^k}) = 0$$

$H(i_1 \,||\, i_2 \,||\, \ldots \,||\, i_{2^k})$ начинается с d нулевых битов.

Изначально задуманный как ASIC-устойчивый, Equihash является квантово-устойчивым в том смысле, что классические устройства для его реализации экономически эффективнее квантовых, поэтому исключается возможность концентрации больших вычислительных ресурсов у атакующего с применением квантовых вычислительных устройств.

Вместе с тем остается характерная для всех Proof of Work алгоритмов проблема централизации классических вычислительных мощностей. Как показывает опыт, ни одна попытка создания ASIC-устойчивых алгоритмов не увенчалась успехом. Алгоритмы Ethash, Cryptonight, Equihash, которые предположительно должны были служить этой цели, в итоге были реализованы в виде интегральных схем специального назначения. Для любого вида вычисления можно создать специализированные устройства, которые будут заточены под конкретную задачу и справляться с ней лучше, чем устройства общего назначения (CPU или GPU).

Наиболее уязвимыми для атаки 51% являются криптовалюты с небольшим хешрейтом, которые копируют алгоритм майнинга у другой криптовалюты с большим хешрейтом. На примере *Equihash*(n = 200, k = 9): чтобы произвести атаку двойной траты, любой небольшой майнинговый пул Zcash, на котором сосредоточено несколько процентов мощности сети, может на незначительное время незаметно для участников пула переключить часть мощностей на добычу блоков в другом блокчейне с тем же алгоритмом, но с достаточно низкой вычислительной мощностью. Таким способом в 2018 году были атакованы Bitcoin Gold, Zencash и, скорее всего, будут атакованы все остальные криптовалюты с небольшим хешрейтом, работающие на популярных алгоритмах *Equihash*(n = 200, k = 9) и *Equihash*(n = 144, k = 5).

Для доказательства выполненной работы в BPQ используется Equihash с параметрами $n = 96$, $k = 3$ (которые на данный момент являются уникальными) в качестве вычислительной головоломки и хеш-функция SHA2-256 для регулирования её сложности.

5. Конфиденциальность

Конфиденциальность является обязательным свойством денег. Никто не имеет права знать, сколько денег лежит в вашем кошельке, когда, кому и за что вы платите, пока вы сами не посчитаете нужным раскрыть кому-то эту информацию.

Изначальная ориентация Биткойна на анонимность публичных ключей и их регулярная смена для достижения конфиденциальности [26] не оправдала себя, так как связи между использованными публичными ключами видны в блокчейне и легко поддаются анализу.

Некоторые криптовалюты пытаются решить данную проблему, используя неинтерактивные схемы доказательства владения с нулевым разглашением такие как zk-SNARKs. Также интерес представляют предложенные схемы конфиденциальных транзакций и MimbleWimble, но данные решения не являются квантово-устойчивыми, поэтому не могут считаться безопасными. Кроме того, важно понимать, что все анонимные транзакции, которые на сегодняшний день делаются с применением квантово-небезопасных алгоритмов, в будущем при необходимости будут легко вскрыты квантовым компьютером, поэтому не могут считаться в полной мере анонимными уже сегодня.

В последующих обновлениях протокола для обеспечения конфиденциальности будут использоваться квантово-безопасные неинтерактивные доказательства с нулевым разглашением наподобие ZKB++/Picnic [27] и zk-STARKs [28].

6. Ссылки

[1] Cryptography Today
http://web.archive.org/web/20151116013105/https://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml

[2] IBM Q Experience https://quantumexperience.ng.bluemix.net/qx/experience

[3] Intel Bets It Can Turn Everyday Silicon into Quantum Computing’s Wonder Material
https://www.technologyreview.com/s/603165/intel-bets-it-can-turn-everyday-silicon-into-quantum-computings-wonder-material/

[4] Experimenting with Post-Quantum Cryptography
https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html

[5] Commercialize quantum technologies in five years
https://www.nature.com/news/commercialize-quantum-technologies-in-five-years-1.21583

[6] OpenSSH 7.7 adds experimental support for PQC XMSS keys
https://www.openssh.com/txt/release-7.7

[7] Microsoft Adds Post-Quantum Cryptography to an OpenVPN Fork
https://www.bleepingcomputer.com/news/microsoft/microsoft-adds-post-quantum-cryptography-to-an-openvpn-fork/

[8] D. Deutsch. Fabric of reality. Chapter 2 “Shadows”
https://www.amazon.com/Fabric-Reality-Parallel-Universes-Implications-ebook/dp/B005KGJX8E/

[9] D. Deutsch. The Beginning of Infinity. Explanations that Transform the World. Chapter 11 “The Multiverse”
https://www.amazon.com/Beginning-Infinity-Explanations-Transform-World-ebook/dp/B005DXR5ZC/

[10] D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. https://people.eecs.berkeley.edu/~christos/classics/Deutsch_quantum_theory.pdf

[11] P. Shor. Algorithms for Quantum Computation: Discrete Log and Factoring
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.53.4485&rep=rep1&type=pdf

[12] L. Vandersypen, M. Steffen, G. Breyta, C. Yannoni, M. Sherwood, I. Chuang. IBM Almaden Research Center. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance http://cryptome.org/shor-nature.pdf

[13] J. Proos, C. Zalka. Department of Combinatorics and Optimization University of Waterloo. Shor’s discrete logarithm quantum algorithm for elliptic curves.
https://arxiv.org/pdf/quant-ph/0301141v2.pdf

[14] M. Roetteler, M. Naehrig, K. Svore, K. Lauter. Microsoft Research, USA. Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms
https://eprint.iacr.org/2017/598.pdf

[15] How many bitcoins are vulnerable to a hypothetical quantum attack?
https://medium.com/@sashagnip/how-many-bitcoins-are-vulnerable-to-a-hypothetical-quantum-attack-3e59e4172e8

[16] L. Grover. A fast quantum mechanical algorithm for database search. https://arxiv.org/pdf/quant-ph/9605043.pdf

[17] Post-quantum cryptography. http://pqcrypto.org/

[18] PQCRYPTO. Initial recommendations of long-term secure post-quantum systems. http://pqcrypto.eu.org/docs/initial-recommendations.pdf

[19] J. Buchmann, E. Dahmen, A. Hülsing. XMSS – A Practical Forward Secure Signature Scheme based on Minimal Security Assumptions. https://eprint.iacr.org/2011/484.pdf

[20] A. Hülsing, D. Butin, S. Gazdag, J. Rijneveld, A. Mohaisen. XMSS: eXtended Merkle Signature Scheme. RFC 8391. https://datatracker.ietf.org/doc/rfc8391/?include_text=1

[21] SPHINCS: practical stateless hash-based signatures http://sphincs.cr.yp.to/

[22] A. Hülsing. W-OTS+ Shorter Signatures for Hash-Based Signature Schemes. https://huelsing.files.wordpress.com/2013/05/wotsspr.pdf

[23] Blockchain: how a 51% attack works (double spend attack) https://medium.com/coinmonks/what-is-a-51-attack-or-double-spend-attack-aa108db63474

[24] D. Bernstein. Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete? https://cr.yp.to/hash/collisioncost-20090517.pdf

[25] A. Biryukov, D. Khovratovich. Equihash: Asymmetric Proof-of-Work Based on the Generalized Birthday Problem. https://www.cryptolux.org/images/b/b9/Equihash.pdf

[26] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. Section 10 “Privacy” https://bitcoin.org/bitcoin.pdf

[27] M. Chase, D. Derler, S. Goldfeder, C. Orlandi, S. Ramacher, C. Rechberger, D. Slamanig, G. Zaverucha. Post-Quantum Zero-Knowledge and Signatures from Symmetric-Key Primitives. https://eprint.iacr.org/2017/279.pdf

[28] E. Ben-Sasson, I. Bentov, Y. Horesh, M. Riabzev. Scalable, transparent, and post-quantum secure computational integrity. https://eprint.iacr.org/2018/046.pdf