RANDOCUBE
White Paper

2017

Содержание.

«Генерация случайных чисел
слишком важна, чтобы
оставлять её на волю случая»
русский перевод, автор Robert Coveyou

1. Введение в проблематику. Случайности не случайны.

Для многих людей выбор решений происходит случайным способом. На волю случая люди отводят достаточно большое количество решений. В сети проводят розыгрыши, блогеры используют сервисы генерации случайных чисел для создания интерактивного контента и рекламы. Случай определяет в спорте порядок начала игры. Некоторые споры решаются случайным выбором и порой случай определяет весьма серьёзные последствия.

В игорной индустрии остро стоит проблема доверия пользователей к сервисам-рандомизаторам. Невозможно доказать и невозможно опровергнуть случайность полученных значений для розыгрышей, казино, лото и т.д. Проблема заключается ещё и в том, что вы играете против организатора и организатор, отдавая выигрыш, несёт убытки из собственного кармана. Возникает конфликт интересов. Для достижения прибыльности создаётся система с максимально низкими шансами на выигрыш, с подставными игроками и конечно с махинациями случайного значения.

Многие существующие рандом сервисы в интернете предоставляют искусственный генератор случайных чисел. Такие генераторы основаны на математических алгоритмах лишенных физической возможности создать по-настоящему случайную комбинацию. Генераторы псевдослучайных чисел воспроизводят энтропию из базового заданного значения. Такой метод не безопасен и используется из-за легкости реализации. Таким образом сгенерированное число не совсем случайно и не имеет подтверждения. Некоторые сервисы описывают свои генераторы случайных чисел как высокоэнтропийные аппаратные генераторы случайных чисел. Но не один из сервисов не может доказать, что их генератор вообще существует.

Мы решили создать универсальный инструмент, имеющий высокую степень энтропии и доказывающий реальность, и честность полученных значений. Мы создали свой собственный аппаратный генератор случайных чисел (АГСЧ)* и добавили в него возможность подтверждения. Основное решение проблемы заключается в том, чтобы генерировать случайные значения совместно с доказательством процесса генерации. Пользователь получит комбинацию из доказательства и результата генерации источника энтропии. Мы назвали это системой подтвержденного аппаратного генератора случайных чисел (ПАГСЧ). В дальнейшем в поисках оптимальных решений для построения системы мы определили понятие ПАГСЧ.

Система подтвержденного аппаратного генератора случайных чисел - это аппаратный генератор случайных чисел, в котором каждое новое число проходит процедуру подтверждения социально общепринятой регулярно обновляющейся информацией за счёт одновременной записи и трансляции происходящих процессов.

В основе метода подтверждения мы применяем технологию потокового подтверждения данных - Streaming Data Confirmation. Этот принцип позволяет обеспечить прозрачность демонстрируемых данных за счет потоковой трансляции процесса создания новых данных на фоне регулярно обновляющейся социально общепринятой информации.

Этот документ детально описывает базовое решение проблемы доверия в системах требующих доказательство случайности и подтверждение данных.

Решение описанное нами имеет технические недостатки и не является “панацеей”. Но позволяет сформулировать принцип и последовательность решения проблемы доверия в генерации случайных чисел. Мы создали прецедент настоящего доказательства случайности.

Мы занимаемся дальнейшей разработкой протокола потокового подтверждения данных - Streaming Confirmation Protocol (SCP). Спецификация этого протокола отдельно опубликована на GitHub и является открытой и общедоступной. [15]GIHUBLINK Этот протокол не придёт на смену модели Randocube и разрабатывается параллельно с целью создания прозрачных инструментов использования генераторов случайных чисел. И мы надеемся, что эта разработка позволит опираться пользователям на сформулированные нами требования к публичной генерации случайных значений в сети.

*АГСЧ - аппаратный генератор случайных чисел - устройство, которое генерирует случайные числа из физического процесса. [1]

2. Определение предоставленного метода.

Создание случайного числа должно быть доказано сообществу. Лучший способ доказательства это демонстрация процесса вживую. В результате принято решение использовать прямую трансляцию видео происходящего процесса. Видеохостинг YouTube позволил технически реализовать прямой эфир для генерации чисел. Эти действия не просто записываются, они транслируются площадкой, которой доверяют и смотрят миллионы людей.

Для доказательства реальности показанных данных происходит демонстрация общепринятого явления совместно с процессом генерации. В качестве общепринятого явления можно использовать различные природные явления (сейсмическая активность, изменения магнитных колебаний, погодные изменения), эфир теле-радио передач, и ещё множество различных процессов. В нашем ПАГСЧ в качестве одного из доказательств процесса генерации используется график курса валют. Курс валютных пар записывается навсегда и в любой момент времени изменяется под действием множества факторов. Изменения в такой системе всегда можно проверить и проконтролировать.

Randocube является платформой, в которой транслируется видео получения нового числа и формирование графика курса валют в прямом эфире в качестве социально общепринятого информационного потока для подтверждения демонстрируемых данных.

Техническая реализация истинно случайного числа потребовала создание физического объекта. Программные решения не способны решить проблему, потому что любой закрытый код находящийся на стороне сервера может содержать в себе «жульнические поправки» и не способен генерировать высокую энтропию. Специальные платы генераторов случайности и различные датчики использующиеся в компьютерах, не могут наглядно показать процесс создания. Демонстрировать результат аппаратных генераторов приходится через закрытое программное обеспечение на стороне сервера, честность которого доказать невозможно.

Randocube использует физический объект для построения системы доказанной генерации случайности.

В качестве источника энтропии применяется кубик игральных костей. Выбор который определил и название и суть проекта. Случайность генерируемая кубиком

не подлежит сомнению, его физические свойства неизменны. Этот физический объект имеет высокую степень энтропии за счёт свободного падения тела. Вероятность просчета результата определяется очень большим количеством факторов: свободное падение, случайный отскок, начальная энергия в момент броска, положение при броске и т.д. Все перечисленные факторы изменчивы и математическая модель конструкции Randocube, не может быть эффективной, даже при высокой степени детализации.

Мы активно вовлечены в процесс разработки прямого использования blockchain в построении специальной сети подтвержденной генерации энтропии. Технология blockchain становится общепризнанной и совмещение Randocube с blockchain является естественным продолжением развития проекта.

3. Определение степени энтропии для Randocube.

Для определения качества энтропии, мы использовали тест-эксперимент. В ходе эксперимента непрерывно сгенерировано 200000 значений. [2] Исходя из процентного соотношения полученных значений мы определили результат распределения. Процент максимального расхождения в значениях не превышает 0,01 %.

Распределение значений на установленный период в 200000 генераций имеет ровный характер без ярко выраженных перекосов, что означает высокую степень случайности.

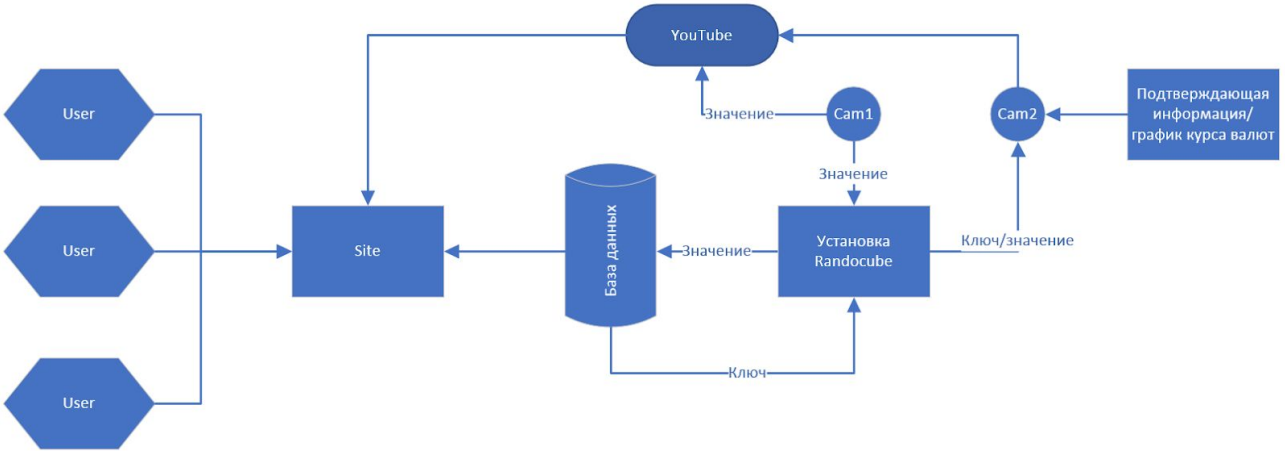
4. Randocube. Принцип работы устройства.

Randocube должен быть понятным и открытым, максимально приближенным к естественным процессам. Для этого сконструировано специальное устройство, позволяющее циклически с высокой точностью выполнять смену значений и при этом наглядно демонстрировать результат.

Для чтения данных и подтверждения используются две камеры, одна считывает значения, вторая осуществляет подтверждение в реальном времени, снимая изображение на мониторе и процесс генерации случайных значений в одном кадре так, чтобы полученные данные можно было сопоставить.

Для считывания данных и их записи был разработан алгоритм распознавания чисел с кубика игральных костей. Кубик предоставляет всего шесть вариантов. Но этого оказалось достаточно. Один бросок способен генерировать значение для многих сервисов. Платформа Randocube позволяет обеспечить множество различных интернет ресурсов настоящими случайными значениями. Бросок транслируется в прямом эфире, записан на видео, его результат доступен каждому и каждый может убедиться в реальности его создания. Randocube позволяет работать с указанным диапазоном значений, диапазон не ограничивается значениями игрального кубика. Эта функция реализована с помощью специального алгоритма и использует несколько значений (бросков).

На момент написания этого документа Randocube является установкой подбрасывающей игральный кубик с шестью значениями, в составе которой присутствуют две камеры. Одна камера считывает полученное значение и транслирует видеопоток в Youtube. Вторая камера снимает и через компьютер транслирует на видеохостинг Youtube в прямом эфире весь процесс броска на фоне монитора с графиком курса валют с текущей датой и временем. Трансляция подтверждения с Youtube и результаты считанных значений отображаются в режиме реального времени на сайте Randocube.com. В результате получается аппаратный генератор случайных чисел с подтверждением результатов через веб трансляцию с использованием общепринятой регулярно обновляющейся информацией.



В Randocube используется оборудование, которое работает в режиме 24/7. В таком режиме работы возможны отказы оборудования. Время простоя в случае сбоя будет минимальным, однако сама возможность поломки обязательно должна учитываться при использовании нашей платформы в текущей версии.

Весь процесс создания подтвержденных значений занимает определённое время. Время затрачивается на бросок,, считывание значения, отправку данных в БД, формирование уникального ключа и возврат его в систему Randocube. Далее возникают задержки времени вызванные передачей видеопотока и синхронизацией этого потока со значениями на сайте.

В Randocube реализовано множество различных функций:

- Диапазон чисел. Эта функция позволяет получить случайное значение в указанном диапазоне.
- Розыгрыши для социальных сетей - это возможность провести розыгрыш в автоматическом режиме для блоггеров и компаний с аудиторией из соц. сетей и

Youtube. Предусматриваются различные фильтры, такие как комментарии, репосты, защита от повторов и т.д.
- API для внешних сервисов. Любой может подключить данные из Randocube для своего проекта и использовать уникальный подтвержденный генератор случайных значений для взаимодействия с общественностью.
- Ключ броска. Для удобства поиска состоявшегося процесса генерации мы применяем специальный ключ броска. Ключ генерируется с каждым броском, отображается в видеотрансляции и указывается в таблице сгенерированных результатов. Этот ключ позволяет безошибочно определить результат и способствует доказательству реальности генерации случайных значений так как воспроизводится в видеотрансляции вместе с данными подтверждения. Ключ может быть использован сторонними сервисами для формирования запроса на искомый бросок. (https://randocube.com/result/key/%7Bkey%7D/html)
- При проведении розыгрыша или простой генерации значений присутствует функция сохранения результата и формирования ссылки для полученного значения, эту ссылку можно отправить другим пользователям или использовать для публикации результатов розыгрыша.

5. Алгоритм формирования числа свыше 6, и работа с установленным значением рандома.

Формирование числа свыше шести, в системе из одного кубика происходит за счёт нескольких бросков и специального алгоритма.

Алгоритм определения случайного числа в установленном диапазоне свыше 6:

Принцип алгоритма заключается в разделении диапазона на шесть частей (поддиапазонов) и приведения границы диапазона к максимально возможному кратному шести. Остаток распределяется среди поддиапазонов в зависимости от выпавшего числа, следующие числа определяют распределение остатка и выбор поддиапазона. Финальный бросок сводится к определению значения из последнего выбранного поддиапазона. В случае если размер последнего поддиапазона меньше шести добавляются недостающие поддиапазоны сформированные из имеющихся значений.

Пример 1 реализации алгоритма на диапазоне чисел от 1 до 100.

Общий диапазон от 1 до 100 приводится к максимальному числу кратному шести, в данном примере число равно 96. Это число делиться на шесть частей, в каждой из которых 96/6 значений. Далее определяется и распределяется остаток. Остаток находится исходя из того, что разница нижнего и верхнего предела диапазона должна учитывать все варианты и учитывать сами числа открывающие диапазон, соответственно в формулу добавляется единица. ((100+1-1)−96=4. Число 4 равномерно распределяется в зависимости от первого выпавшего значения смещая значения частей поддиапазонов.

Первый бросок определяет поддиапазон с которого начинается распределение остатка, при этом происходит смещение во всех частях диапазона.

1...16 **17...32+1** **33...48+1** **49...64+1** **65..80+1** **81..96**

Второй бросок определяет поддиапазон в котором продолжится поиск числа. Выбранный поддиапазон снова делится на 6 частей.

1...16 **17...33** **34...50** **51...67** **68...84** **85...100**

Третий бросок определяет поддиапазон с которого будет производится распределение остатка. Остаток выбранного поддиапазона равен пяти (17-33+1)=17, 17-12=5. Где 12 максимальное кратное 6-и число. Если при распределении остатка в поддиапазоны имеется остаток, то распределение продолжается с первого поддиапазона, пока остаток не будет распределен полностью. При смещении поддиапазонов граничные значения поддиапазонов смещаются и соответственно значения смещаются и в следующих поддиапазонах.

17...18+1 **19...20** **21...22+1** **23...24+1** **25...26+1** **27...28+1**

Четвертый бросок выбирает поддиапазон. Выбранный поддиапазон оставшихся значений составляет всего три значения 22, 23, 24. Поддиапазон меньше 6 и кратен 6, соответственно дальнейший выбор будет сделан между двумя значениями кубика на одно число поддиапазона. Значения 1 и 2 будут означать 22, значения 3 и 4 будут означать 23, значения 5 и 6 будут означать 24.

17...19 **20...21** **22...24** **25...27** **28...30** **31...33**

Пятый бросок делает финальный выбор сгенерированного числа.

22 **22** **23** **23** **24** **24**

Результат 24

Пример 2 реализации алгоритма на диапазоне чисел от 1 до 4, в случае если первый бросок генерирует число выше 4.

При таком соотношении формируются недостающие два поддиапазона из основных чисел диапазона. В результате при выборе числа из сформированного поддиапазона потребуется провести еще один бросок для окончательного выбора.

Первый бросок определяет поддиапазон или число. В приведенном примере число 5 определяет, что выбор будет происходить в поддиапазоне от 1 до 2.

1 2 3 4 1...2 3...4

Второй бросок определяет конечный выбор.

1 1 1 2 2 2

Результат 1

6. Решаемые проблемы. Социальный эксперимент.

Randocube - решает несколько фундаментальных проблем:

- *Впервые в сети интернет реализует доказанную генерацию случайности.*

Проблема отсутствия доказанной генерации случайности доведен до предела. Бесконечные интернет казино открыто используют алгоритмы обхода системы мартингейла, и даже не думают о доказательстве рандома, и полностью управляют значениями для каждого пользователя. В медийном бизнесе розыгрыши проводят без реального подтверждения полученных данных, зачастую среди подставных лиц. Создание самой концепции независимого сервиса настоящей подтвержденной генерацией случайных чисел будет перестраивать все перечисленные виды бизнеса на новую прозрачную платформу.

- *Решает проблему доверия между игроками и сервисами;*

Можно быть уверенным, что сервисы использующие систему генератора случайных чисел с подтверждением Randocube предоставляют истинный результат. Вопросы отпадают сами по себе, когда на экране присутствует видео подтверждения выпавшего значения. Это беспрецедентный уровень доверия между пользователями и сервисами.

- *Позволяет удостовериться в истинно случайном выборе.*

Ответственность за выбор очень часто заставляет нас сомневаться в себе. Порой выбор приходится делать из абсолютно идентичных вариантов или в ситуациях когда оценить выбор невозможно. Очень часто неудачи к которым приводит неверный выбор огорчают нас и заставляют чувствовать вину за этот выбор. Это происходит потому, что выбор не был случайным и появляются

сомнения. Используя сервис Randocube каждый может быть уверен, что принятые решения действительно случайны и на них ничто не могло повлиять.

- *Создаёт фундамент для построения новых систем для подтвержденных генераторов случайных чисел.*

Randocube открывает невероятные возможности. Технология потокового подтверждения данных позволяет формировать доказательства различных процессов требующих публичного признания и находящихся на общественном контроле.

- *Создаёт новую модель взаимоотношений между пользователями в сети.*

До выпуска Randocube в мире не существовали системы подтвержденной генерации случайных чисел. Реакция пользователей и действия мошеннических сервисов будут представлять результат социального эксперимента. И могут послужить аналогиями при моделировании других социальных процессов с похожим спектром изменений.

7. Randocube и SDC.

Создавая Randocube мы вкладывали свои силы и средства. Но столкнувшись со множеством проблем поняли, что есть предел наших финансовых возможностей, который сильно ограничил и урезал идею, и мы не могли воплотить её в первоначальном виде.

Сейчас Randocube работает с привычными базами данных и предоставляет API для других сервисов. Все сгенерированные значения и график доказательства привязываются к времени по Гринвичу. Процесс генерации представляет собой последовательность действий:

- Бросок;
- Определение значения;
- Запись в бд;
- Возврат ключа броска для отображения в трансляции.

Эта версия будет служить столько времени, сколько потребуется. Дальнейшее развитие идеи возможно с развитием протокола потокового подтверждения данных.

Протокол основан на совмещении изменяющейся общепринятой информации и децентрализованной системы хранения данных. Такая концепция позволит фиксировать процессы произошедшие в реальности и являющиеся частью реальной истории. Разработка этого протокола позволит публиковать информацию и не требовать доказательств работы, опираясь исключительно на поток.

8. Применение.

Мы видим платформу Randocube как естественную часть сообщества и рассматриваем взаимоотношения людей в обществе с учетом экономической составляющей. Важнейший фактор живучести любой идеи это положительный экономический эффект. Randocube потенциально способен изменить рекламный рынок, а продукты на основе Randocube способны повлиять на игорный бизнес.

Размещение рекламы:

Randocube это платформа и продукт одновременно. Мы позволяем использовать наши данные для построения новых сервисов и при этом предоставляем собственные сервисы, для розыгрышей в частности. Розыгрыши и другие интерактивные акции проводятся многими успешными контент мейкерами и разнообразными площадками и группами. В первую очередь это большой пласт контекстной и интегрированной рекламы с прямым откликом аудитории. Наше

взаимодействие через Youtube и другие социальные каналы как Telegram открывает доступ к этой аудитории. Randocube может предлагать рекламные включения через площадки блогеров, блогеры и медийные проекты смогут проводить розыгрыши честно и без нареканий со стороны аудитории.

Взаимодействие с игорным бизнесом:

Рандокуб способен повлиять на постоянно растущий игорный бизнес и сделать его более честным, многие участники этого рынка просто не имеют альтернативы для реализации прозрачных площадок. Они пользуются управляемым рандомом, и не понимают как доверие может пробудить интерес к индустрии в целом и продуктам в частном. Рандокуб позволяет открыть новые возможности для взаимодействия и привести с собой честных участников рынка.

9. Randocube Team.

Команда Randocube это энтузиасты свободы и равноправия. Мы выступаем за самоорганизованное общество. Наш продукт создан с целью сбалансировать общество и дать новые возможности, для открытого и прозрачного взаимодействия людей. Мы не сторонники создания раздутого штата, у нас много друзей и мы привлекаем их по мере необходимости.

Tarasov Artem - Chief technology officer (CTO).

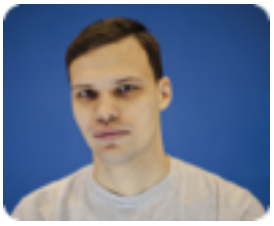
Руководитель направления электронного конструирования. Имеет богатый опыт в создании электронных устройств.

Работал в автомобильной промышленности. Руководит строительно монтажными работами в области безопасности и средств связи.

Nikishenkin Andrey - Chief Design Officer (CDO), Chief Program Officer (CPO).

Руководитель разработки программного обеспечения. Руководитель разработки дизайна.

Работал в автомобильной промышленности. Работал над обработкой и визуализацией данных конструкторских измерений геометрии автомобилей. Опыт в разработке desktop и web-приложений более 8 лет.



Evdeshin Vladimir - Chief Operating Officer(COO).

Руководитель развития компании Randocube. Разработчик программного обеспечения электронных устройств.

Руководил проектом систем безопасности и связи. Работал инженером-программистом.

10. Вывод.

Randocube - является первой в мире платформой с доказательством генерации случайности, и наша команда будет продолжать развитие этой идеи. Мы верим в то, что в обществе всегда должен быть островок справедливости, честности и свободы. Когда-то таким местом стал интернет, он стал вторым домом для многих людей и позволил находить единомышленников по всему миру. Randocube платформа свободная для использования, которой могут доверять все. В интернете обязательно найдется место для свободного и по настоящему честного генератора случайности - Randocube.

Randocube при поддержки сообщества сможет вытащить гигантский пласт проблем и разрешить большинство из них. Сообщество нуждается в этих решениях и наша команда пришла к такой идеи не случайно. Мы столкнулись с этими проблемами в повседневной жизни. И чем дальше углублялись в причины происходящего, тем больше понимали, что зреет необходимость в решении. Мы уверены в том, что наше решение правильное, возможно оно не идеально, но для этого мы обращаемся к сообществу. Каждый участник Randocube помогает сделать его лучше, и решить годами накопившиеся проблемы недоверия и злоупотребления генерацией случайных значений в обществе.

Artem Tarasov
Andrey Nikishenkin
Vladimir Evdeshin

Источники:

1. https://ru.wikipedia.org/wiki/Генератор_псевдослучайных_чисел
2. https://en.wikipedia.org/wiki/Pseudorandom_number_generator
3. https://theethereum.wiki/w/index.php/ERC20_Token_Standard
4. https://bitcoin.org/bitcoin.pdf
5. https://ru.wikipedia.org/wiki/Аппаратный_генератор_случайных_чисел
6. https://www.groupm.com/news/groupm-global-ad-investment-will-grow-43-in-2018-six-countries-to-drive-68-of-incremental-investment
7. https://www.prnewswire.com/news-releases/research-and-markets---worldwide-gambling-market-to-reach-635-billion-2016-2022-drivers-opportunities-trends-and-forecasts---key-vendors-are-888-bet-at-homecom-betfair-bwinparty-ladbrokes-paddy-power-and-unibet-300334698.html