!<---BEGIN AUTHOR PUBLIC KEY--->!

0xAE8A7aC2358505a11f51c7a1C1522D7b95Afe66F

!<---END AUTHOR PUBLIC KEY--->!

!<---BEGIN AUTHOR NAME--->!

Берланд Юрий Михайлович/Berland Yuriy Michaelovich/born. 18.08.1992

!<---END AUTHOR NAME--->!

Cryptiber - сервис для подтверждения авторства для документов с целью защиты интеллектуальной собственности.

Автор: Юрий Берланд

Аннотация

Регистрация авторства на изобретение или художественное произведение путем подтверждения прав на исходный файл. Предложенный нами механизм основывается на устойчивости криптографической хеш-функции, что позволяет существенно сократить трудозатраты и обойтись без посредников. Так же это позволяет авторам регистрировать свои изобретения и открытия, не разглашая их и не обращаясь к посредникам. Мы создаем данный механизм с целью возможности справедливого вознаграждения непосредственных авторов того или иного произведения за свой труд, а так же увеличение скорости выхода инноваций на рынок засчет сокращения времени и издержек на подтверждение авторства.

Введение

На сегодняшний день защита интеллектуальной собственности сталкивается с целым рядом трудностей: юридические услуги по её оформлению часто дорогостоящие и долгие в реализации. Это, в свою очередь, приводит к тому, что многие разработчики или авторы оказываются не в состоянии подтвердить свои авторские права самостоятельно, что может привести к тому, что правообладателем изобретения становится лицо, не вложившее в разработку свой труд, вознаграждение за который и должно обеспечивать авторское право.

По этой причине выпуск многих изобретений и медийных продуктов тормозится из-за опасения авторов относительно "кражи", т.е. присвоения авторских прав.

Кроме того, постоянно возникает опасность присвоения результата интеллектуальной деятельности до того, как право на них оформлено юридически. В процессе между фактическим созданием информации, представляющей ценность и юридическим оформлением прав на неё, о ней может узнать множество посредников: деловые партнеры, сотрудники компании, контрагенты и просто случайные люди. Любой из них может присвоить себе авторство, либо нежелательно распространить сведения.

Основная причина подобной ситуации кроется в необходимости в квалифицированном посреднике, аналогичная причине, повышающей стоимость платежей (особенно трансграничных), для снижения которой и был первоначально задуман биткоин [1], созданный Сатоши Накамото именно с этой целью.

Регистрация авторства

Предлагаем механизм, позволяющий быстро и с минимальными трудозатратами засвидетельствовать свое авторство над тем или иным информационным продуктом. Это может быть как патент на изобретение или технологическое решение, так и художественное произведение, текст песни, портфолио и т. д. В основе метода лежит электронная цифровая подпись, криптографическая хеш функция и регистрация в цепочке блоков, снабженных меткой времени [1].

Общая схема работы выглядит так: авторский контент записывается в стандартизированный файл, включающий в себя так же и информацию о публичном ключе автора, используемом для подтверждения его прав среди участников сети, а так же о его личности, чтобы подтвердить свои права при разрешении спора в классической правовой системе.

В общем виде это может выглядеть так:

!<---BEGIN AUTHOR PUBLIC KEY--->!

1DJA3b7dTknHeM3xfpZWUgWwzuFLs8MGLf

!<---END AUTHOR PUBLIC KEY--->!

!<---BEGIN AUTHOR NAME--->!

Pushkin Alexander Sergeevich

!<---END AUTHOR NAME--->!

Мой дядя самых честных правил,

Когда не в шутку занемог,

Он уважать себя заставил

И лучше выдумать не мог.

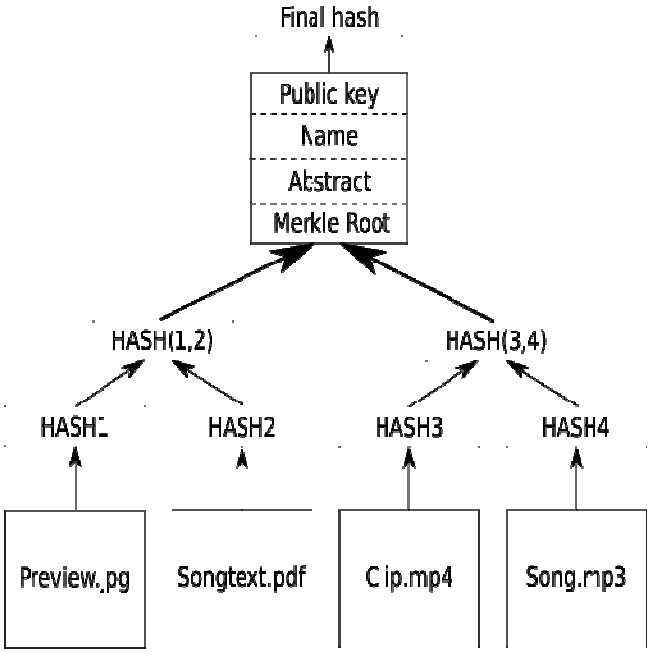
В реестре, исполненном в виде цепочки блоков будет храниться только хеш сумма данного файла, а сам контент становится известным участникам только тогда, когда автор захочет доказать свои права. При этом на его ответственности остается сохранение файла в неизменном виде с точностью до 1 бита, в противном случае хеш сумма оного изменится, и автор уже не сможет ничего доказать [3].

Для этой цели рекомендуется вычислять хеш сумму и сохранять в неизменном виде информацию в формате .pdf или распознаваемой картинкой, в отношении которой соблазн её "немного подправить" будет значительно меньше.

При этом если мы говорим о желании заверить авторство над графическим контентом, то это так же можно сделать, вычислив хеш суммы всех прилагаемых фото, видео, аудио и иных файлов, после чего в заверяемый файл сохраняются все эти хеш суммы, либо их общий корень дерева

Меркла. В любом случае, на автора ложится ответственность за сохранность не только хешируемого файла, но и всех используемых приложений (рис.1).

Рис.1. Пример для видео клипа:



Таким образом, автор сохраняет возможность доказать свои права на произведение или изобретение до тех пор, пока у него хранятся:

1. Собственный приватный ключ (электронная цифровая подпись), соответствующий указанному в сохраненном файле публичному ключу.

2. Подтверждение личности (не обязательно при решении спора исключительно внутри сети)

3. Хешируемый файл в виде, неизменном с момента вычисления его хеш суммы

4. Все файлы-приложения, так же неизменные с момента вычисления корня дерева Меркла и/или хеш суммы каждого из них (если они имелись изначально)

На сегодняшний день уже имеется прецедент подтверждения факта того или иного высказывания

Наличие метки времени позволит доподлинно установить время, когда был создан авторский контент. Это значительно поможет в разрешении споров. Заметим так же, что хеш сумма неразрывно связана как с самим контентом, так и с идентификационными данными автора. В случае, если злоумышленник захочет засвидетельствовать уже записанный ранее контент, но со своими идентификационными данными, ему придется перебирать все возможные варианты записи авторства, будет оставаться практически невозможно даже когда в цепочке блоков будет суммарно значительное количество свидетельств. Так например, если будет появляться 20 новых свидетельств ежесекундно, то за 10 лет их число достигнет 2^{32}, тогда как если использовать SHA256 для их вычисления, нужно будет перебрать все 2^{256} комбинаций, что практически невозможно[6].

Транзакции

Для оплаты услуг по записи своего контента в очередном блоке цепи используется внутренняя цифровая валюта (так называемые марки сети Cryptiber, рекомендуемое обозначение CryptiberMark, CBM), выплачиваемая создаелю блока. По мнению автора, валюту сети уместнее всего сравнивать с почтовыми марками.

Сами марки выпускаются по классическому механизму доказательства выполнения работы, описанному Сатоши Накамото. При этом транзакции ничто не мешает размещать в тех же блоках, что и записи об авторстве (свидетельства).

Если транзакции впоследствии могут храниться в виде корня дерева Меркла, то свидетельства должны храниться у всех участников сети вечно. Для этого мы разделяем их на два типа:

1. Транзакции типа "TO" - для передачи марок (или токенов сети) другому участнику. Общий вид:

"OWNER1" TO "OWNER2" 1.00000 width 0.00100

Данная запись гласит, что владелец 1 передал владельцу 2 1 марку с комиссией 0.001 марки. В данном случае комиссия может устанавливаться добровольно и может быть практически нулевой при низкой загруженности сети. в реальной цепочке блоков в качестве записей "OWNER1" и "OWNER2" указываются их публичные ключи (адреса).

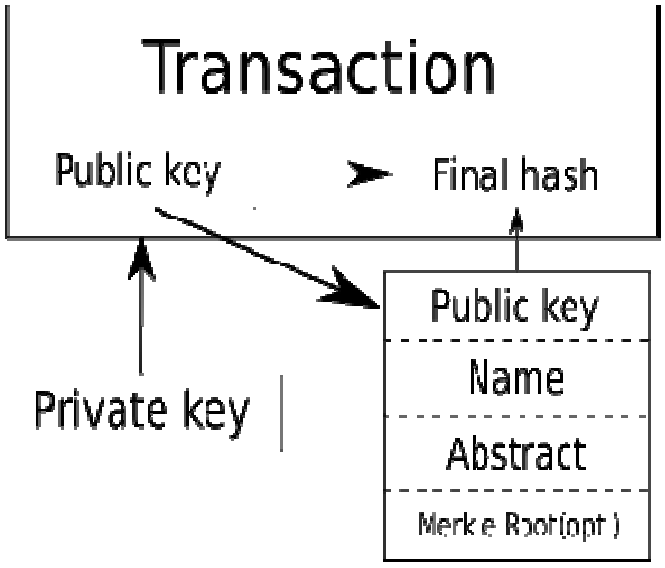
2. Транзакции типа "FOR" - служат непосредственно оплате регистрации авторства. Общий вид:

"OWNER1" FOR "FinalHash(file.pdf)" 1.00000

В данном случае получателя получатель отсутствует, а сумма транзакции целиком переходит создателю блока за публикацию записи. Важно, чтобы владелец в качестве своего публичного ключа указывал в хешируемом файле тот же ключ, что и указан как отправитель транзакции. Это позволит легко подтвердить свое авторство транзакцией на любую сумму с того же адреса.

Общий вид транзакции для регистрации авторства показан на рис. 2.

Рис. 2. Общий вид транзакции - регистрации авторства:



В данном случае комиссия обязательна в размере не менее 1 марки. Это не должно вызывать затруднений у большинства населения: первоначально 100 марок будет продаваться за $1 при

максимальной эмисссии 84 млрд штук. Даже при массовом использовании и значительном (до 1 к 1) подорожании стоимость услуги остается ничтожно мала по сравнении с классическими услугами посредников при регистрации авторских прав.

Возможно так же указание префикса для транзакции, указывающего на односторонне разрешенные автором пределы использования, например:

CC - Creative Commons - автор разрешает свободно пользоваться заверенным контентом

PT - Проприетарное - автор разрешает пользование контента с его согласия на возмездной основе

PTXX - Проприетарное, с указанием запрашиваемого автором процента от прибыли за пользование контентом, вместо XX подставляется процент: PT06 - 6%, PT20 - 20% и т. д. При этом следует считать приоритетным договор между автором и пользователем, если таковой имеется в виде контракта и/или смарт-контракта.

Общий вид:

"OWNER1" FOR "FinalHash(file.pdf)" 1.00000 CC

"OWNER2" FOR "FinalHash(text.pdf)" 1.00000 PT15

Доказательство авторства

Поскольку в цепочке блоков хранится не полный текст оригинального файла, а только его хеш, авторство будет оставаться неизвестно до тех пор, пока автор не заявит о своих правах. Когда же он это делает, ему достаточно предьявить исходный файл судье или другому доверенному лицу. При отсутствии доверия к решающему спор допускается выложить исходный файл с информацией для проверки публично. Вычисляя его хеш, он видит его присутствие в блоке.

Далее проверяется соответствие публичного ключа внутри хешируемого файла с ключом отправителя транзакции за его регистрацию в блоке. Его личность так же может быть подтверждена сверкой данных из файла с данными, подтвержденными документально.

Недостаток здесь в том, что посредник, будучи человеком или закрытой программой, может быть скомпрометирован злоумышленником путем подлога, подкупа или иными методами. В таком случае он заявит, что хеш невалидный и откажет в признании авторства за заявителем.

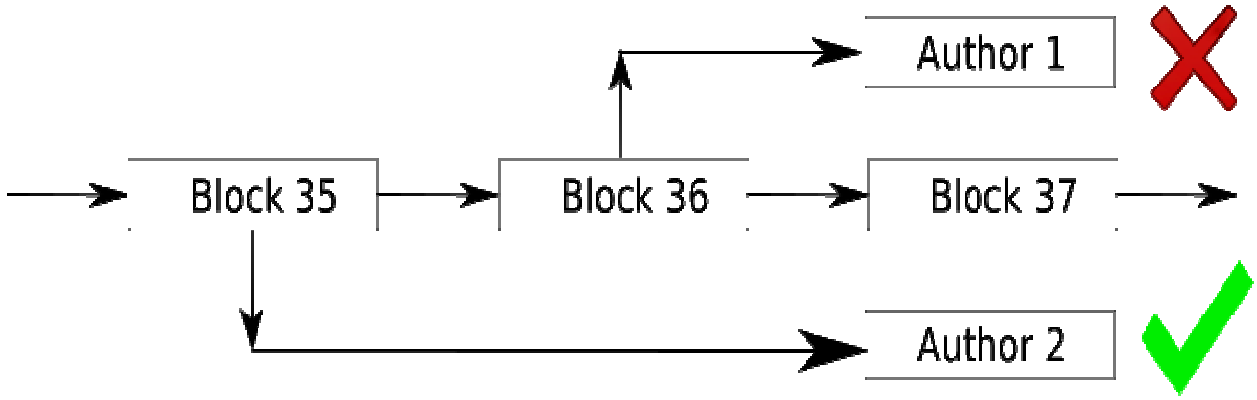
В таком случае, исходный файл может быть показан множеству проверяющих (размещен в открытом доступе). Поскольку в обозримом будущем количество проверяющих (не более населения Земли и/или количества вычислительных устройств) будет много меньше числа возможных вариантов хеша (так например, количество IP-адресов IPv6 может быть не более 2^{60} против 2^{256} вариантов SHA256), если валидный хеш смогла получить группа лиц достаточно многочисленная, чтобы её участников можно было считать не связанными между собой, однозначно можно сделать вывод о том, что они получили его вычислением хеш-суммы валидного исходного файла, предоставленного автором. На практике с большой вероятностью они и составят большинство в случае, если случайное произвольное редактирование файла перед вычислением его хеш-суммы будет хоть сколько-либо трудозатратной.

Обратите внимание, что данная группа может не обязательно составлять большинство проверяющих, что делает систему более надежной: даже контроль над большинством возможных

участников сети исключает возможность для злоумышленника отрицать авторство честного участника сети (автора), опубликовавшего валидный исходный файл.

Следующая опасность состоит в том, что новый пользователь, увидевший работу уже с заверенным авторством, захочет присвоить авторство себе. Для этого он копирует заверенный уже контент, создает новый файл со своей личностью и публичным ключом и заново его регистрирует. В таком случае будет достаточно сравнить два (или более) заверенных документов, означающих фактически одно и тоже, и посмотреть, какой из них заверен в более раннем блоке. Это и будет подтвержденный автор (Рис. 3).

Рис. 3. Автором признается заявитель, заверивший авторство в более раннем блоке:



Наконец, поскольку регистрируется только хеш-сумма документа, исходный документ может содержать в себе что угодно, в том числе слова и фразы, явно не представляющие ценность как результат интеллектуальной деятельности. В таком случае, необходим уже консенсус в сообществе.

Если в контентной части заверенного документа содержатся исключительно общие формулировки, не упрощающие создание того или иного продукта (например "миру мир" или "давайте жить дружно"), то он может быть заверен, но никаких правовых последствий за этим не последует.

Чтобы автор мог на что-либо претендовать, ему необходимо заверить авторство над документом с подробным описанием продукта, либо полностью или большей частью художественного произведения. Важно понимать, что необходимость повторного вычисления хеш суммы каждый раз будет означать невозможность внести даже минимальные изменения в документ без необходимости заново заверять его авторство. В этом и состоит страховка от подобных действий со стороны сети.

Государственная регистрация авторства очень трудозатратна, поэтому регистрации и подлежат только документы и материалы, прошедшие проверку цепочкой посредников. В нашем случае регистрируется только компактная хеш сумма документа, что и позволяет обойтись без сложных процедур на этапе регистрации.

Правовое обоснование

Запуская данный проект, мы не дожидаемся законодательной инициативы, направленной на его использование. При этом мы приходим к выводу, что мы поступаем правильно, а законодательная инициатива неизбежно последует за повсеместным использованием озвученных нами методов.

В соответствием с конституциями большинства развитых стран высшим органом власти выступает народ, под которым на практике понимается совокупность граждан того или иного государства. В нашем случае это означает, что повсеместное использование нашей программы неизбежно повлечет за собой признание со стороны государственных структур.

Стоит так же заметить, что технология блокчейн и криптовалюта первоначально так же не имели под собой правовой базы, что не помешало им обрести ценность среди заинтересованных в её существовании граждан, что в конечном итоге привело к законодательным инициативам, большинство из которых в конечном итоге оказалось нацелено на её регулирование, нежели на запрещение.

На сегодняшний день уже известны прецеденты использования свидетельских показаний в качестве доказательства авторства. [7] Законодательство большинства современных государств предусматривает авторство над любым результатом интеллектуальной деятельности по факту его создания. Таким образом, надежный механизм доказательства последнего неизбежно повлечет за собой его признание.

Мы делаем вывод о том, что благодаря общественному мнению и судебным прецедентам (в том числе с участием судов присяжных) предложенная нами модель доказательства авторства, основанная на криптографии, неизбежно найдет отражение в законодательстве и в судебной практике, если ей будут пользоваться повсеместно.

На сегодняшний день в судебной практике признается только государственная регистрация авторских прав. Однако, практически повсеместно в судебной практике учитываются свидетельские показания.

Автор вполне может лишится патента, если в ходе судебного процесса будет доказан факт кражи изобретения. В нашем же случае количество свидетелей может исчисляться миллионами - это все пользователи, обладающие копией всей цепочки блоков. Каждый из них в случае публикации валидного исходного файла будет знать настоящего автора в купе с датой регистрации им авторства с точностью до нескольких минут.

В таких условиях попытка отстоять "свое" авторство злоумышленником становится чрезвычайно затруднительно. Даже если это ему удастся, остается постоянный риск того, что авторство за другим человеком будет впоследствии доказано задним числом, что даст последнему право не только требовать передачи всех прав ему, но и возмещения ему всех убытков, включая упущенную выгоду.

Столь высокие риски для злоумышленника, злоупотребляющего действующей правовой системой, делают более целесообразными переговоры с автором, первым заверившим свой труд по представленной нами или аналогичной схеме.

Особенно высоки перспективы данного проекта в странах англо-саксонской правовой семьи (США, Великобритания), где развито прецедентное право.

Заключение

В данной статье мы предлагаем механизм, позволяющий непосредственному автору изобретения, книги, песни или любого другого продукта, подтвердить свое авторство быстро, практически с нулевыми затратами и, самое главное, без необходимости разглашения своего продукта третьим лицам до регистрации.

Механизм подходит для любого информационного продукта:

- Патент на изобретение или технологический процесс
- Стихотворение или песня
- Картина
- Фильм или любое видео
- Книга или сценарий
- Просто идея, если она достаточно подробно изложена и не очевидна и многое другое.

Низкие издержки позволяют регистрировать даже шутки, анекдоты, афоризмы, публикации в социальных сетях и тому подобное. Это помогает авторам в свободном распространении материала: по скольким рукам ни разошлась бы публикация, первоначальный автор всегда сможет доказать свои права.

Криптография в нашем случае позволит заверять авторство, в том числе, и над документами, составляющими государственную или коммерческую тайну: их содержание может оставаться известным для всех кроме непосредственных участников проверки.

Еще одно положительное последствие внедрения нашей системы мы видим в перераспределении доходов от интеллектуальной собственности от правообладателей, ставших таковыми в результате отчуждения прав, в пользу непосредственно фактических авторов оной. В долгосрочной перспективе это приведет к снижению стоимости результатов интеллектуальной деятельности в купе с повышением их качества и скорости внедрения.

Человек, заверивший авторство предложенным нами способом, может размещать потом материал где угодно, но доказательство все равно останется за ним.

Ссылки

1. Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf

2. ГК РФ, статья 1257. Автор произведения. http://www.consultant.ru/document/cons_doc_LAW_64629/7dde8dbb10c5ce94297e5eb859712be091044d70/

3. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf

4. Brad Templeton. A brief intro to copyright. https://www.templetons.com/brad/copymyths.html

5. Chinese #MeToo Student Activists Use Blockchain to Fight Censors https://www.bloomberg.com/news/articles/2018-04-24/chinese-metoo-student-activists-use-blockchain-to-fight-censors

6. Florian Mendel, Tomislav Nad, Martin Schlaffer Improving Local Collisions: New Attacks on Reduced SHA-256 https://online.tugraz.at/tug_online/voe_main2.getvolltext?pCurrPk=69018

7. ОДИННАДЦАТЫЙ АРБИТРАЖНЫЙ АПЕЛЛЯЦИОННЫЙ СУД 443070, г. Самара, ул. Аэродромная, 11А, тел. 273-36-45 www.11aas.arbitr.ru, e-mail: info@11aas.arbitr.ru ПОСТАНОВЛЕНИЕ апелляционной инстанции по проверке законности и обоснованности решения арбитражного суда, не вступившего в законную силу: http://kad.arbitr.ru/PdfDocument/54747d58-47c2-4b3f-9994-ce3e6d05d789/aa703915-ffae-4e9d-a10a-6f67cb545b9a/A65-12697-2015_20160212_Postanovlenie_apelljacionnoj_instancii.pdf

8. Арбитражный суд Республики Татарстан. Дело № А65-12697/2015 http://kad.arbitr.ru/PdfDocument/54747d58-47c2-4b3f-9994-ce3e6d05d789/72cfa586-8f7d-4dba-8be4-afd95efcf6fc/A65-12697-2015_20150925_Reshenie.pdf

9. Poor man's copyright http://www.copyrightauthority.com/poor-mans-copyright/

10. How Do You Notarize If A Signer Can’t Be Present? https://www.nationalnotary.org/notary-bulletin/blog/2016/11/how-to-notarize-if-signer-cant-be-present

11. Credibility of witnesses. www.nycourts.gov/judges/cji/1-General/CJI2d.Credibility.pdf

12. Croatia considers Bitcoin legal. https://99bitcoins.com/croatia-considers-bitcoin-legal-45-members-of-the-swiss-parliament-want-the-same/