ПОЛНОСТЬЮ РАСПРЕДЕЛЕННЫЙ ПРОТОКОЛ GRIDNET, БЕЗ ДОВЕРЕННЫХ АВТОРИТЕТОВ

Rafal Skowronski
Department of Computer Science
Poznan University of Technology, Poland
rafal.skowronski@cs.put.poznan.pl

***Аннотация*— Обмен информацией между людьми в современном мире имеет огромное значение. Людям требуется передавать данные, но при этом им также необходимо сохранять где-то большие куски данных для последующего обращения. Была создана целая индустрия, обеспечивающая такую возможность. В некоторых случаях, предоставляется необходимая инфраструктура – кабели или беспроводные базовые станции GSM/LTE, в других случаях – обеспечиваются дополнительные возможности хранения (облачные службы хранения). В этой статье мы рассмотрим ПОЛНОСТЬЮ РАСПРЕДЕЛЕННЫЙ протокол *GRIDNET* (*FD-GRIDNET*). Он позволяет мотивировать пользователей для того, чтобы они приняли участие в обмене данными. В качестве целевой среды рассматриваются сети MANET/DTN, но мы не хотим ограничивать использование данного протокола только в этих сетях. *FD-GRIDNET – это первый полностью распределенный протокол обмена данными, который вознаграждает посредников криптовалютой, созданной в описываемой здесь коммуникационной системе.* Он представляет собой систему коммуникации с замкнутым экономических циклом, где тот, кто выступает в роли "роутера", зарабатывает криптовалюту, которая, в свою очередь, может использоваться для внутренних нужд, например – для трансмиссии данных. *FD-GRIDNET*, можно сказать, основана на использовании криптовалюты. Она построена на концепте POW, но также использует и POS.**

Keywords— mobile networks; Ad-hoc networks; Disruption tolerant networks,consensus, cryptocurrency, P2P

I. INTRODUCTION

Военно-воздушные силы США, пытаясь разработать систему, которая переживет ядерную атаку, создали глобальную вычислительную сеть. [9]. В конце 80-х годов, из-за коммерциализации технологии коммутации, произошел переход от сетей с коммутацией каналов к сетям с коммутацией пакетов. И где-то в это время появился стек протоколов TCP/IP – основа сети INTERNET – глобальной сети, предназначенной для обмена пакетами данных, с которой мы очень хорошо знакомы сегодня.

Глобальные системы контроля за данными больше не являются предметом теоретических спекуляций. Это – уже факты (PRISM) [10,11]. У человека должен быть выбор, с кем он или она хочет поделиться своими частными данными – пусть даже это метаданные.

На данный момент, возможность цифровой коммуникации зависит исключительно от телекоммуникационных компаний. Хотя существующая система, в общем случае, практически полностью обеспечивает текущий потребности в коммуникации и достаточно широко распространена в городских районах, в ней по-прежнему имеются недостатки, связанные с доверием. Правительство многих стран вынуждает телекоммуникационные кампании записывать все сеансы общения, или, по крайней мере, обеспечивать хранение коммуникационных событий – метаданных. Более того, во многих сельских районах отсутствует необходимое оборудование; поэтому, там просто отсутствует возможность легкой коммуникации на больших расстояниях. С целью обеспечения возможности недорогой связи. Было разработано множество протоколов и проектов; включая различные типы MANET или варианты коммутации каналов в сочетании с аппаратными средствами (WI-FI). Однако, большинство этих методов не обеспечивают должным образом конфиденциальности, безопасности, и того, что наиболее важно – универсальной системы вознаграждения посредников. Для решения этой проблемы было выдвинуто множество предложений. Некоторые из них основаны на репутации, другие – на экономических решениях; но ни одно из них не предлагает использовать универсальный токен, который можно было бы использовать не только при обмене данными, если такая необходимость возникнет Более того, ни одно из них не предлагает такой механизм консенсуса, который позволил бы обходиться без необходимости доверия третьим сторонам.

Мы полагаем, что ретрансляционные узлы – основа всех распределенных сетей с коммутацией пакетов, и, чтобы они участвовали в процессе по своей воле, им должны быть предоставлены определенные стимулы. В общем, сотрудничество в мобильных сетях ad-hoc, также, как и в любом другом типе сетей, - где ретрансляционные узлы являются автономными – не дает никаких преимуществ от участия в распределении данных. Узлы могут управляться различными авторитетами, имеющими разные приоритеты. Чтобы сэкономить батарею, сохранить пропускную способность и мощность обработки, узлы могут пытаться пересылать как можно меньше пакетов другим. Если значительное количество узлов выберет такую стратегию, то качество сети значительно ухудшится для всех.

Поэтому необходима полностью распределенная система коммуникации, которая будет вознаграждать посредников

на основе переданного ими объема данных. Эта коммуникационная система не должна иметь никаких доверенных третьих сторон, должна быть надежной и устойчивой к различного рода атакам и недостойному поведению.

Но мы нашли решение. Итак, представляет вашему вниманию *протокол FD-GRIDNET* - первую полностью распределенную систему коммуникации, основанную на базе данных с распределенным реестром, также известную как “блокчейн”. Мы используем как POW, так и POS. Механизм POW (proof-of-work) уже был использован в различных криптовалютах – например, *Bitcoin* [6], который проложил путь другим. Биткоин использовал концепт POW, чтобы достичь консенсуса относительно состояния базы данных распределенного реестра, содержащую транзакции между пользователями. Следует отметить, что при использовании системы коммуникации, предоставляющей справедливое вознаграждение посредникам, особое внимание следует уделять передаче пакетов. Каждый поток данных в *FD-GRIDNET* через блокчейн. Никакие переданные данные нигде не сохраняются, а идентификаторы коммуникации полностью анонимны. Специализированные узлы проверяют коммуникационные потоки и ретранслируют тикеты. Побочный продукт процесса, являющийся виртуальной валютой, распределяется между ретрансляционными узлами в соответствии с их вкладами. В нашей схеме, для минимизации ужасного стимулирования, а также для обеспечения более высокой пропускной способности сети, используется POS; POS, в данном случае, лучше POW. Каждый пользователь должен предъявить определенное доказательство работы, связанное с идентификацией, перед тем, как принять участие в работе сети. Это доказательство затем будет служить как доказательство доли (POS). Когда нода начинает “химичить”, то она потеряет свой стейк.

В итоге, мы предлагаем первую полностью распределенную систему коммуникации, которая позволяет решить проблему вознаграждения посредников за их работу и использование их ресурсов. Мы также решаем проблему обработки некорректных нод и оптимизируем принятие решений на основе голосования и POS. В различных источниках было высказано достаточно много идей о том, как взаимодействовать с некорректными нодами. При этом, мониторинг и схемы, связанные с репутацией, стоят достаточно недешево. Также требуется “подслушивание” передач от других. Чтобы изучить различные решения более подробно, обратитесь к работе Сони и Джина [1].

Благодаря высокому уровню обобщения, у нашего протокола довольно широкий спектр использования – от различных облачных решений, где ноды вознаграждаются за предоставление возможности хранения данных, до одноранговой системы обмена данными. Самое интересное, что наш протокол позволяет создать анонимную коммуникационную сеть, участие в которой оплачивается. *FD- GRIDNET* подходящий выбор как для развертывания сети в беспроводном варианте, так и для использования поверх интернета.

Marti, Giuli, Lai и Baker [7] обсуждают ретрансляцию нод без переадресации. Имеются и другие предложения, большинство из которых слишком оптимистичны, - например, если ретраснлирующая нода не “прослушивает” другой после определенного количества повторных передач пакетов в течение заданного количества времени, то отправитель уведомляется о неисправности ноды. Однако, здесь не учитывается той возможности, когда множество нод объединяется для атаки на легитимные ноды, чтобы уничтожить их, вызвав “Отказ в Обслуживании”. Также сложно найти защиту от случая, когда нода из черного списка генерирует новую идентификацию сразу после исключения. Если каждая нода будет хранить информацию о репутации, то как мы сможем синхронизировать информацию? И как мы узнаем, не передает ли злоумышленник пакеты с ложной информацией? В предыдущих работах упор делался на отдельных аспектах, поэтому эти работы оказываются слишком непрактичными. SORI [2] описывает алгоритмы обнаружения эгоистичного поведения, обеспечивающие безопасность и использующие цепочку хэшей для распространения данных о репутации. Однако это эффективно только тогда, когда ноды статичны, и данные о репутации будут распространяться среди постоянных, неподвижных участников. Из-за отсутствия глобального источника информации, новые ноды, появляющиеся поблизости, остаются неизвестными. Совершенно очевидно, что одна из главных проблем заключается в отсутствии защиты от размножения новых идентификаций сразу после исключения.

Идея экономического стимулирования либо определенной оплаты услуг посредников не нова [3], [4], [5]. Тем не менее, все существующие предложения требуют либо определенного аппаратного обеспечения с безупречной проверкой [2] либо доверенных авторитетов [4], [5]. В нашем случае, система гарантированно обеспечивает распространение данных в соответствие с назначенным набором правил при условии, что честные ноды контролируют больше мощности ЦПУ, чем любая взаимосвязанная группа нод-злоумышленников.

II. ФОРМУЛИРОВАНИЕ ПРОБЛЕМЫ

Сформулируем проблему следующим образом. Допустим, мы хотим, чтобы нода A отправила ноде B данные через произвольное количество посредников. При этом, только нода B должна иметь возможность расшифровать данные. Чтобы улучшить защиту от статистического анализа, ни один из посредников или получателей данных не должен знать путь, по которому шла передача данных. Благодаря этому, посредники не смогут обманывать систему стимулирования, например, путем добавления произвольного количества посредников к датаграмме с целью увеличения прибыли. Также, ни один посредник не сможет удалить предыдущих посредников из списка задействованных нод, чтобы украсть или максимизировать прибыль. Система выплатит вознаграждение только после успешной доставки данных.

При этом, должны соблюдаться следующие ограничения:

- Каждая нода не должна иметь симметричной связи с любой другой нодой. После обмена данными между посредниками, информация о посредниках должна уничтожаться.

• Ноды должны быть работоспособны и иметь возможность принимать правильные решения о маршрутизации (ретранслировать или нет, оплачивать транзит или нет) даже без доступа к общему блокчейну.

• Ни один посредник не должен иметь информации о получателе, и не должен знать, передает ли он датаграмму фактическому получателю или нет

• Мы не хотим разрешать обмен данными, если у источника данных нет средств покрыть расходы. Но нужно учесть, что за один раз может передаваться очень большое количество пакетов данных. Проверка каждого пакета на то, есть ли средства у отправителя, создаст большие задержки и расходы. Поэтому необходимо добиться возможности проведения одной проверки для конкретного потока данных

• Получатель данных не должен иметь возможности вступить в сговор с отправителем данных для бесплатной передачи данных

• В любой заданной точке должна обеспечиваться полная безопасность

Еще нет такого протокола, который соответствовал бы всем заданным критериям.

III. POW и POS

Общеизвестно, что чем более ограничен запас валюты, тем выше ее стоимость; цена регулируется обычно искусственным образом.

В нашем протоколе, в качестве стимула выступает криптовалюта, имеющая ограниченную поставку. Чтобы предоставить доказательство выполнения работы (POW) при обработке блока транзакций, нужно потратить определенное время и энергию (в форме электричества). Когда кто-то зарабатывает криптовалюту, он может использовать ее для генерации токена трансмиссии (TT). TT служит для посредников доказательством того, что отправитель готов оплатить передачу данных. TT можно рассматривать как некую финансовую облигацию, не имеющую определенных владельцев. Тем не менее, каждый посредник имеет возможность проверить ее подлинность и, при сотрудничестве, получить по ней свою долю.

Но никто не хочет рисковать больше ожидаемого дохода от инвестиции. Именно здесь в игру вступает POS – доказательство доли владения. Каждая нода должна вычислить POW своего идентификатора. Это POW состоит из значения хэша, числовое представление которого должно быть ниже определенного порога, определяемого как трудность работы. POW сочетается с nonce – одноразовым кодом, выбранным случайным или псевдослучайным образом, который используется для безопасной передачи основного пароля, предотвращая атаку повторного воспроизведения. В случае переполнения, адрес соединяется сам с собой, пока не будет достигнут успех. То, что появляется в результате, служит как *Proof-Of-Stake*. Он сохраняется в блокчейне вместе с адресом, и присоединяется к каждой датаграмме, сгенерированной данным адресом. В случае отсутствия выплат от источника данных или в случае его неправильного поведения, нечестная нода потеряет свои стейки – она потеряет исходное доказательство работы, подсоединенное к его адресу.

IV. ТОКЕНЫ ТРАНСМИССИИ (TT) И ПУЛЫ TT

Пул токенов – структура данных, представленная хэш-цепочкой. Единый пул токенов определяется 100-битным значением хэш-сида SHA256, количеством хэшей, присутствующих в хэш-цепочке, и самым крайним значением данной хэш-цепочки.

Существуют также поля, связывающие данный хэш-пул с адресом владельца и отсылающие к транзакции, которая относится к монетам, использованным для

генерации пула токенов. Так как хеш-пул вычисляется человеком, жертвующим монеты, то этот человек – единственный, кто знает хеш-значения между частичным хеш-сидом и максимальным хеш-сидом. Исходный хеш-сид останется секретом до тех пор, пока не будет исчерпан. Количество известных битов сида достаточно для того, чтобы избежать коллизий (ноды благодаря этим битам определяют конец значения токена); в то же время, скрытая часть достаточна для того, чтобы избежать взлома. Окончательный хеш может и должен быть публично известен. Монеты, пожертвованные для генерации пула, не исчезают бесследно. Каждый отдельный хеш, или диапазон хешей из родительского пула токенов, могут быть использованы при создании единого токена передачи.

Токен Трансмиссии (TT) – структура данных, посредством которой источник данных разрешает передачу датаграммы.

Рисунок 2:Токен трансмиссии, подписанный отправителем

Так как пул токенов генерируется благодаря использованию определенной суммы криптовалюты; поэтому каждый хеш в пуле токенов – доля в этой сумме. То есть, при отправке криптовалюты на безвозвратный адрес, происходит обмен монет на хэши

[1] Валюта не уничтожается, а депонируется для будущих посредников

в пуле хешей. . Значение хеша в данном хеш-пуле можно вычислить следующим образом

$$\frac{\text{Количество пожертвованных монет}}{\text{Количество хешей в хеш-пуле}}$$

Одиночная датаграмма присоединяется к одиночному токену трансмиссии. При этом указывается награда за трансмиссию *(TR)*. Одиночный *TT* может ссылаться на одиночный хеш из пула токенов или диапазона хешей, указывая при этом количество обнаруженных хешей. Таким образом, создатель данных может установить приоритет датаграммы. Чем выше TR, тем больше стимула у посредников хранить и передавать информацию. С другой стороны, постепенно уменьшающаяся прибыль для других посредников будет препятствовать тому, чтобы сеть была “затоплена” старыми нерелевантными датаграммами. Это облегчает функционирование механизма *Time-To-Live*, который регулирует спрос и предложение.

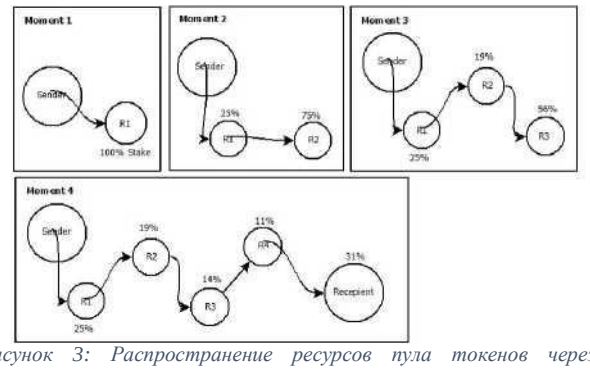

Рисунок 3: Распространение ресурсов пула токенов через токен трансмиссии

На рисунке 3 показано, как награда за трансмиссию распределяется среди посредников. Когда датаграмма достигает первого посредника, то этот посредник получает в распоряжение полную долю *TR*. Когда текущая нода решает осуществить трансмиссию данных другой ноде, то она также передает 75% награды другой ноде. Далее все повторяется. Поэтому недопустимо, чтобы текущая нода добавляла искусственные, принадлежащие ей самой, адреса для выплат в список переходов (иначе она получит все вознаграждение). С другой стороны, каждая нода “знает”, что, наиболее вероятно, ей необходимо передать данные, так как ей неизвестна в точности целевая нода. К тому же, время – тоже существенный фактор. Создатель данных может быть достаточно богат, чтобы нанять множество исходных мессенджеров. Поэтому, следует учесть, что награду получит только тот, кто успешно доставит данные – и именно те посредники, которые были в данной успешной цепочке. Ниже будет описано, как защитить список переходов от нечестных действий.

V. ХРАНЕНИЕ ИНФОРМАЦИИ КАК ЧАСТЬ РАСПРЕДЕЛЕННОГО БЛОКЧЕЙНА, ДЕРЕВЬЯ МЕРКЛА, ДОСТИЖЕНИЕ КОНСЕНСУСА

В нашей системе, любая важная информация хранится как часть распределенного реестра. Каждая запись в реестре – блок. Блоки связаны друг с другом – каждый следующий блок содержит хеш-значение предыдущего. Чем больше блоков, тем сложнее злоумышленнику заменить конкретный блок. Сложность здесь заключается в требуемой вычислительной мощности, так как данные, находящиеся внутри блока, должны содержать хеш, соответствующий определенному критерию сложности, то есть, он должен быть ниже определенного значения. Полные ноды – ноды, хранящие весь блокчейн – соперничают друг с другом, пытаясь найти правильный nonce – уникальное значение внутри блок. Хеш блока всегда будет ниже предельной сложности. Выигрывает блок с наивысшей сложностью – он принимается другими нодами и добавляется в блокчейн. Таким образом, достигается консенсус между различными майнящими нодами. Поэтому атака потребует большой вычислительной мощности. Чем больше блоков, тем безопаснее блокчейн.

Есть полные ноды – те, которые хранят полный блокчейн, и есть лайт-ноды. Полные ноды проверяют транзакции; для этого нужна большая вычислительная мощность. Лайт-ноды являются полностью функциональными нодами; они не хранят всего блокчейна, и при необходимости запрашивают данные.

Основа отдельного блока - дерево меркла, которое, в свою очередь, содержит десятки транзакций. Когда лайт-нода хочет проверить транзакцию, ей не нужно запрашивать весь блокчейн или даже весь блок. Ей лишь нужно запросить у полной ноды путь внутри дерева меркла, содержащий проверяемую транзакцию.

Теперь давайте остановимся на том, как типичный механизм POW относится к нашей схеме. Основное различие в способе проверки полными нодами транзакциями. В нашем случае, полные ноды проверяют как транзакции, так и информационные потоки. Необходимо, чтобы полные ноды “осознавали”, что имеется криптовалюта, депонированная для будущих посредников, и что им может потребоваться “выкупить” этот депозит. Вот одна из главных причин, почему в *FD-GRIDNET* не может быть реализована мета-валюта[2]. В нашем видении, информационные потоки определяются токенами трансмиссии.

Каждая полная нода определяет, использовался ли данный хеш в определенном хеш-пуле. Может возникнуть ситуация, когда хеш из более глубокой, то есть близкой к сиду, части хеш-пула уже использовался для другой трансмиссии. Каждая нода отслеживает состояние использования текущего хеш-пула. К счастью, для хранения хеш-пула необходима эффективная память. Хеш-пул, подходящий для отправки 100.000.000 датаграмм, состоит из 256-битного хеш-сида, 256-битного конечного хеша, и целого числа. В случае повторного использования хеша, данная нода заносится в черный список в блокчейне; таким образом, она не сможет больше передавать датаграммы.

VI. СТРУКТУРА ДАТАГРАММЫ и ПЕРЕДАЧА ДАННЫХ

В *FD-GRIDNET* нет инфраструктуры *PKI*. Распределенный блокчейн служит как глобальный источник доверенной информации, а его целостность защищена механизмом POW. Пользователи идентифицируются их адресами. Адреса выводятся из публичных ключей пользователей.Частные ключи хранятся в секрете и никому

[2] Metacurrency – криптовалюта, основанная на уже установившемся блокчейне (например, блокчейне BITCOIN).

не доступны. Каждая датаграмма содержит анонимный адрес отправителя.

Рисунок 4: Пример идентификации POW

Sample Identity Proof of Work
Sender address: 1BvBMSGYstWetqTFn5Au7m4GFg7xJaNVN
nonce: 123456789
number of concatenations:0
friendlyID: user1
proof-of-work:
000000000000006bc28cb4165ff97fb2b193b79e7496ad605662ea5f4b4d1b90

В сценарии, где нет доступа к полной ноде, то есть, к блокчейну, подтверждение POW для посредников происходит путем проверки идентификатора отправителя (рисунок 4). Каждый токен трансмиссии подписан, поэтому, в случае повторного использования TT либо указания несуществующего пула токенов, отправитель будет забанен как только адресат начнет оформление доставки.

Награда посреднику рассчитывается как часть награды за трансмиссию. Поэтому, получатель может согласиться обслуживать одного отправителя не так часто – для получения максимально возможной прибыли. Это приведет к сокращению блокчейна и позволит получателю и посредникам получить прибыль. Каждый посредник может бесплатно проверить состояние своей выплаты в блокчейне. Если выплаты в разумные сроки не произойдет, то посредник может прекратить пересылать датаграммы для данного пользователя.

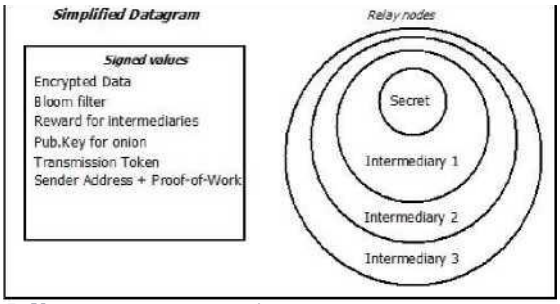

Рисунок 5: Упрощенная структура датаграммы

L

Датаграмма *FD-GRIDNET* состоит из двух ключевых частей. Первая часть подписывается диспетчером. Она содержит фильтр блума – используется для принятия решений о маршрутизации, токен трансмиссии, адрес отправителя – в сочетании с хэшем, удовлетворяющим определенному POW; в нем также указана награда для посредников. Публичный ключ внутри фрагмента данных датаграммы очень важен. Он используется посредниками при добавлении своих адресов в список ретрансляционных нод. При уменьшении списка происходит повторный сбор onion (луковая маршрутизщация), причем каждый слой инкапсулирует адрес одного посредника. Каждая ретрансляционная нода добавляет новый уровень шифрования, используя один и тот же публичный ключ, предоставленный отправителем. Для посредников, как и для получателя, нет возможности узнать или модифицировать предыдущие ретрансляционные ноды. В центре onion имеется секретное значение, генерируемое и известное только отправителю. Это препятствует удалению ноды из списка ретрансляционных нод, или повторному использованию списка для других передач. Конкретный onion валиден только для определенной датаграммы. После разрешения, инициированного получателем, все ожидающие onions передаются полным нодам вместе с соответствующими токенами передачи и секретными значениями. Эти значения включаются в блокчейн. Как только отправитель замечает, что передача одобрена внутри блокчейна, он передает в блокчейн секретный ключ, чтобы полные ноды начали работу по распределению выплат.

VII. ОБСУЖДЕНИЕ БЕЗОПАСНОСТИ, КОНФИДЕНЦИАЛЬНОСТИ И РЕГИСТРАЦИИ FRIENDLYID.

Сегменты данных внутри датаграммы зашифровываются с помощью симметричного шифра; ключевая фраза шифруется при помощи публичного ключа. Публичные ключи хранятся внутри блокчейна. Для получения публичного ключа отправителю необходимо запросить своих соседей – то есть, обратится к блокчейну.

Пользователи могут запросить публичный ключ при помощи FRIENDLYID. FRIENDLYID реализован как своего рода DNS-система внутри блокчейна. Стоит упомянуть, что из-за огромного объема работы, необходимой при генерации POW, привязанной к идентификации, последствия различного вида вредоносного поведения можно смягчить, забанив нечестную ноду на основе различных эвристик путем голосования.

VIII. ОБРАТНАЯ СИТУАЦИЯ

Предположим, нода ищет определенную информацию – например, файл. Она может уведомить соседей об этом факте и предложить награду. Ретрансляционная нода, организовавшая доставку, получает награду.

IX. БУДУЩЕЕ

В настоящее время, мы работаем над реализацией. Мы стараемся лучше сформулировать интеграцию гибридного механизма POW/POS внутри блокчейна для увеличения пропускной способности данных

X. ПРИЛОЖЕНИЯ И РЕЗЮМЕ

Мы предлагаем практическое решение проблемы вознаграждения посредников на основе их работы при использовании блокчейна. Начиная от внедрения внутри сетей MANET/DNT до облачных сервисов хранения.

REFERENCES

[1] Self-Policing Mobile Ad-Hoc Networks by Reputation Systems, Sonja Buchegger, Jean-Yves Le Boude
[2] SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad-hoc Networks
Qi He Dapeng Wu, Pradeep Khosla
[3] L. Buttyan and J. Hubaux, "Enforcing service availability in mobile ad-hoc WANs," IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHoc), Boston, MA, USA, Aug. 2000.
[4] M. Jakobsson, J. Hubaux, and L. Buttyan, "A micro-payment scheme encouraging collaboration in multi-hop cellular networks," Proceedings of Financial Crypto 2003, Gosier, Guadeloupe, Jan. 2003.
[5] S. Zhong, J. Chen, and Y. Yang, "Sprite: a simple, cheat-proof, credit-

based system for mobile ad-hoc networks," IEEE INFOCOM 2003, San Francisco, CA, USA, April 2003.
[6] Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto
[7] Mitigating Routing Misbehavior in Mobile Ad Hoc NetworksSergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker Department
[8] U.S Government, Gold Reserve Act , January 30th 1934
[9] History of Telecommunications Technology, Christopher H. Sterling, George Shiers
[10] Gellman, Barton; Poitras, Laura (June 6, 2013). "US Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program". The Washington Post. Retrieved June 15, 2013.
[11] Braun, Stephen; Flaherty, Anne; Gillum, Jack; Apuzzo, Matt (June 15, 2013). "Secret to PRISM Program: Even Bigger Data Seizures". Associated Press. Retrieved June 18, 2013