Инженерный вестник Дона, №6 (2023)
ivdon.ru/ru/magazine/archive/n6y2023/8482

Децентрализованный реестр данных в технологии суверенной личности

А.С. Акутин, А.В. Бровко

Саратовский Государственный Технический Университет им. Гагарина Ю.А., Саратов

Аннотация: В данной статье рассматриваются вопросы практической реализации системы суверенной личности на базе технологии распределенного децентрализованного реестра данных, также известного, как блокчейн. Приводится реализация системы, основанная на механизме достижения консенсуса Proof of Stake (PoS), обеспечивающая ряд преимуществ по сравнению с альтернативными реализациями, описанными в литературе. Приводятся результаты измерения производительности системы в сравнении с известными реализациями на базе Proof of Work (PoW), подтверждающие высокую эффективность предложенного решения.
Ключевые слова: Децентрализация, ориентация на пользователя, шифрование на основе личности, блокчейн, система суверенной личности.

Введение

В последние годы крайне актуальна тема моделей и методов обработки персональных данных, различные разработки в этой области стремятся решить такие проблемы, как: мошенничество в работе с персональными данными, утечки персональных данных, ошибки в работе antifraud-систем и другие насущные проблемы, возникающие при эксплуатации крупнейших систем, в том числе в управлении в технических отраслях. С одной стороны, проблемы пытается решаться за счет введения новых правовых и юридических норм [1], которые должны защитить пользователей от недоброжелателей. С другой стороны, работы ведутся также в области и технических реализаций и новых подходов к хранению и обработке информации как таковой.

Одним из новых механизмов по работе с персональными данными является подход, называемой “система суверенной личности” (Self Sovereign Identity System, SSI) [2,3]. Данный механизм позволяет выстроить процесс управления цифровой личностью (Identity Management), используя распределенные цифровые реестры данных. Традиционно, говоря о цифровой личности, выделяют три подхода - централизованная модель,

объединенная модель и децентрализованная модель. Последняя форма является ядром, на котором строится система суверенной личности - все данные хранятся у пользователей в зашифрованном виде, история операций публична и находится в децентрализованном реестре (блокчейне), все операции же работают за счет реализации технологии смарт-контрактов.

Найк и Дженкинс в своей работе [4] рассматривали систему суверенной личности как фреймворк с открытым исходным кодом, который уже можно интегрировать в различные сферы жизни. При разработке своей системы авторы указывают, что используют механизм достижения консенсуса Proof of Work (PoW), и отмечают не самую высокую эффективность данного подхода. В настоящей работе ставится задача изучить альтернативные алгоритмы достижения консенсуса в блокчейне применительно к системе суверенной личности и выработать более подходящее решение, разработать прототип механизма достижения консенсуса, а также рассмотреть процесс интеграции блокчейна с выбранным механизмом достижения консенсуса в описанную технологию SSI.

Метод решения

Блокчейн

Рассмотрим технологию блокчейна, как механизм хранения и подтверждения информации, используемый в системе суверенной личности как реестр операций. Блокчейн представляет из себя набор блоков информации, каждый из последующих соединен с предыдущим. Отметим, что в данной работе не рассматривается механизм хранения этих блоков информации, они могут храниться как в оперативной памяти компьютера, так и на жестком диске. Однако, разумеется, говоря о реальных решениях, данные необходимо хранить на жестком диске. Блоки информации ссылаются на предыдущие блоки информации, для более эффективной передачи данных и утилизации вычислительных мощностей используются

хеш-функции. Часто в популярных блокчейн-решениях используется древо Меркла [5] для подтверждения целостности данных. Дерево Меркла представляет собой хэш-дерево и имеет следующие характеристики: листовой узел — это хеш-значение блока данных, и каждый нелистовой узел является хэш-значением дочернего узла. Последний узел называется корнем Меркла. Ко всему прочему, дополнительной и очень важной возможностью дерева Меркла является возможность реализовать механизм подтверждения с нулевым разглашением (Zero-Knowledge Proof) [5].

Механизм достижения консенсуса

В любой распределенной системе существует задача достижения консенсуса - процесса согласования или принятия решения без ведущего узла. На данный момент существует значительное количество алгоритмов, которые позволяют достигнуть консенсуса в распределенном реестре. Количество разработанных механизмов увеличивается с ростом популярности рассматриваемой темы. Разумеется, при создании надежной системы на основе блокчейна следует отдать свой выбор одному из тех, что зарекомендовал себя лучше других и уже используется в работающих решениях. Среди существующих и хорошо работающих алгоритмов можно выделить 2 популярных:

- Proof of Work (PoW)
- Proof of Stake (PoS)

Рассмотрим каждый из алгоритмов по очереди.

Алгоритм Proof of Work был одним из самых первых решений, использованных в блокчейн - решениях. Именно этот алгоритм используется в сети Bitcoin [6], сети, которая стала одной из первых, доказавшей работоспособность данного механизма. Также алгоритм Proof of Work использовался в другой популярный платформе Etherium. Консенсус в

данном подходе достигается за счет случайного подбора числа, удовлетворяющего заранее выбранным условиям. Как следствие - участнику сети, майнеру, как принято называть их в сообществе, необходимо затратить большое количество вычислительных ресурсов на подбор нужного значения, что значительно увеличивает энергозатраты [7] даже целых стран, не говоря уже о конкретных физических лицах.

Пример простого алгоритма Proof Of Work, реализующий подбор случайно-сгенерированного хеш-значения, написанного на языке программирования Python:

```
def valid_proof(last_proof, proof, last_hash):
    """
    Validates the Proof
    :param last_proof: <int> Previous Proof
    :param proof: <int> Current Proof
    :param last_hash: <str> The hash of the Previous Block
    :return: <bool> True if correct, False if not.
    """

    guess = f'{last_proof}{proof}{last_hash}'.encode()
    guess_hash = hashlib.sha256(guess).hexdigest()
    return guess_hash[:4] == "0000"
```

Листинг 1

Алгоритм Proof of Stake [8] является альтернативным подходом [9] в системах распределенного реестра как технология достижения консенсуса. Перед инженерами и учеными, разрабатывавшим PoS-алгоритм, стояла задача решить проблему энергопотребления, обнаруженную в подходе PoW. Получившееся решение позволяет находить консенсус не за счет подсчета

псевдослучайных величин, но за счет траты внутренней валюты сети [10]. Этот подход требует меньше времени на генерацию нового блока и меньшие затраты энергоресурсов.

Интеграция блокчейн в систему суверенной личности

В системе суверенной личности существуют несколько важных действий, которые выполняются основными элементами сети. Для более прозрачного понимания описываемых процессов на рисунке 1 приводится принципиальная схема взаимодействия компонентов системы, состоящая из четырех элементов. Важно отметить, что ядром всей этой системы является блокчейн, на основе него производятся все операции системы.

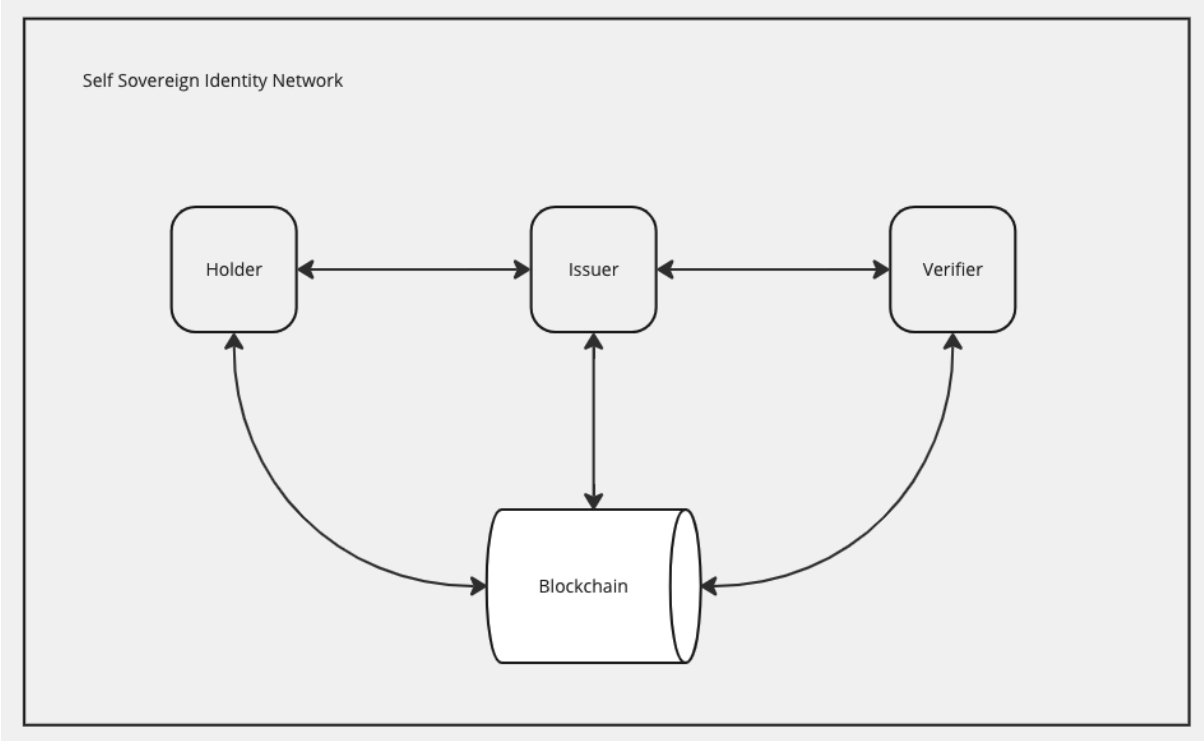

Рисунок 1. – Принципиальная схема взаимодействия компонентов системы

Для работы всей системы необходимы приведенные ниже протоколы, детальный алгоритм которых раскрывается в других

исследовательских работах [11]. Все эти протоколы рассматриваются в контексте накладываемых на них спецификой системы ограничениями:

- Регистрация DID (Decentralized Identifier) - процесс, при котором Issuer выпускает токен определенного содержания и передает его компоненту системы, отвечающему за хранение и использование распределенного идентификатора. В рамках суверенной личности интересующим параметром является скорость генерации новых блоков и количество транзакций в секунду.
- Протокол регистрации Verifiable Credentials - процесс, при котором держатель децентрализованного идентификатора регистрирует в системе свои проверяемые учетные данные. Здесь важно соблюсти высокую скорость генерации новых блоков, что необходимо для работы системы.
- Протокол верификации - самый важный процесс в системе, который позволяет компоненту системы под именем Verifier произвести проверку данных о Holder. Вся информация о результатах проверки хранится в публичном распределенном реестре, потому скорость количество транзакций на единицу времени является критически важным параметром для сравнения.

Ограничения выбора механизма достижения консенсуса

При разработке системы суверенной личности необходимо выбрать алгоритм достижения консенсуса и использовать его в децентрализованном распределенном реестре (блокчейне). Система суверенной личности - механизм, который может существенно упростить решение многих вопросов, связанных с документооборотом, управлением техническими системами и даже некоторых вопросов, связанных с государственными процессами. В отличие от криптовалют, систем перспективных, но очень молодых, здесь необходима надежность, масштабируемость и прогнозируемость. Более того,

сама внутренняя валюта здесь не является ключевой, она - лишь второстепенный продукт, позволяющий использовать сильные стороны блокчейна.

Был реализован алгоритм на языке программирования Golang. Алгоритм состоит из следующих обязательных шагов:

- Участник системы, претендующий на право быть оказаться в блокчейне, делает “ставку” - какое-то количество внутренней валюты;
- Все ставки объединяются в один общий пул (pool) для голосования;
- Каждый участник добавляется несколько раз, пропорционально добавленной стоимости внутренней валюты;
- Псевдослучайным образом выбирается победитель данной лотереи. После этого выбранный узел считается правильным в рамках всей цепочки блоков.

Таким образом, мы тратим внутреннюю валюту, у нас нет необходимости постоянно проводить математические операции с недетерминированным временным исходом. В рамках реализации системы суверенной личности данных подход может быть очень удобен по той причине, что прикладная система, эксплуатируемая в рамках какого-то технического и/или промышленного комплекса, должна быть предсказуемой. Важно упомянуть, что система суверенной личности - механизм, который может эксплуатировать как полноценный продукт в облачной инфраструктуре [11], так и в форме отдельного standalone-решения. Ко всем описанным выше ограничениям стоит добавить потребление энергии, которое необходимо сократить до возможного минимума.

Прототип

Прототип системы реализован на языке программирования Golang, исходные код реализованного алгоритма Proof of Stake можно увидеть на листинге 2 ниже.

```
func PickWinner(Blockchain []model.Block, candidateBlocks []model.Block, validators map[string]int) []model.Block {
    temp := candidateBlocks
    lotteryPool := []string{}
    if len(temp) > 0 {
    OUTER:
        for _, block := range temp {
            for _, node := range lotteryPool {
                if block.Validator == node {
                    continue OUTER
                }
            }
            setValidators := validators

            k, ok := setValidators[block.Validator]
            if ok {
                for i := 0; i < k; i++ {
                    lotteryPool = append(lotteryPool, block.Validator)
                }
            }
        }
        s := rand.NewSource(time.Now().Unix())
```

```
                r := rand.New(s)
                lotteryWinner := lotteryPool[r.Intn(len(lotteryPool))]
                for _, block := range temp {
                        if block.Validator == lotteryWinner {
                                fmt.Println("Winner is: " + block.Validator)
                                Blockchain = append(Blockchain, block)
                                break
                        }
                }
        }
        candidateBlocks = []model.Block{}
        return Blockchain
}
```

Листинг 2

На данном листинге видно, как алгоритм проходит по всем узлам-валидаторам, сделавшим ставку. Дальше формируется массив, состоящий из повторяющихся узлов - количество повторений пропорционально сделанной ставке во внутренней валюте. Можно легко сделать вывод, что чем выше ставка - тем выше шанс на победу в запрограммированной лотерее. Таким образом, возможно достигнуть консенсуса за счет анализа ресурсов (валюты), которыми располагают узлы-валидаторы.

Численные результаты

Метод измерения

В рамках исследования было проведено измерение производительности блокчейнов, реализованных на разных алгоритмах (PoW и PoS). Измерялось время добавления транзакции в блокчейн путем вызова соответствующего метода получения времени в языке golang. Сравнивалось

время, затраченной на добавление 100 транзакций со временем добавления предыдущих 100 транзакций и проводился сравнительный анализ в попытках выявить увеличение скорости производства новых блоков. Сделанные при измерениях допущения:

- Время на генерацию транзакций в реальной системе будет отлично от времени, которое было получено при тестировании. Было сделано эмпирическое предположение, что задержки в сети окажут пропорциональное влияние на оба алгоритма и ими можно пренебречь
- Время, даваемое системой языка программирования может быть неточным, если речь идет о миллисекундах. Поскольку погрешность измерения одинакова в обоих тестах, то было решено ею пренебречь, так как она не оказала бы статистически важного влияния на полученные результаты
- Алгоритм может быть оптимизирован для достижения большей пропускной способности. Задачей работы было провести сравнительный анализ и не стояла задача оптимизации

Полученные результаты

Как описывалось выше, в рамках разработки блокчейна был использован Proof of Stake, который показывается куда как более высокую производительность с точки зрения транзакций в секунду, что было изучено в предыдущих исследованиях на эту тему [12]. В предыдущей работе был рассмотрен анализ растущего времени при производстве транзакций в алгоритме PoW [13]. В работе других исследователей, как они сами и отмечают, используется также алгоритм Proof of Work, что является алгоритмом с прогрессирующей сложностью обработки транзакций [5].

При анализе производительности решения, рассмотренного в текущей статье, не было выявлено усложнения производительности транзакций на 5 млн транзакций, время на 100 транзакций осталось

константным - порядка 20-30 транзакций в секунду (при результате 7-10 транзакций в секунду в алгоритме PoW, в начале работы, до увеличения сложности генерации блока). Ожидаемое для нас знание было получено - мы можем не опасаться увеличения производительности транзакций на единицу времени.

Сравнительный анализ и выбор механизма

Для системы суверенной личности важнейшим фактором, который необходимо учесть при выборе алгоритма достижения консенсуса в распределенном реестре, является скорость генерации транзакций. Полученные результаты демонстрируют, что скорость новых транзакций выше (30 т/с против 7 т/с). Подробный сравнительный анализ можно увидеть в таблице 1 ниже, он составлен из работ других исследователей и полученных в данной работе результатов [8, 9].

Таблица 1 - Результаты сравнительного анализа реализаций PoW и PoS

	PoW	PoS
Скорость генерации транзакций (транзакций в секунду)	7-10	20-30
Требования по аппаратному обеспечению	Наличие видеокарты или специализированных устройств для майнинга	Не предъявляются
Потребление энергоресурсов	Высокое	Обычное
Достижение консенсуса	В зависимости от хешрейта	В зависимости от количества монет

Исходя из сравнительного анализа, стоит сделать вывод, что для реализации описанных выше протоколов в системе суверенной личности лучше выбрать алгоритм PoS.

Выводы

В данной работе рассмотрена технология суверенной личности как принципиального нового подхода по хранению и управлению персональными данными. При подробном рассмотрении децентрализованных реестров и алгоритмов достижения консенсуса в них, было выявлено, что для описываемой технологии алгоритм Proof Of Stake является оптимальным решением для задач получения консенсуса между распределенными узлами, что решает проблемы, заявленные другими исследователями и упомянутые в начале статьи. Также был разработан прототип программы на языке Golang и получены практические данные, подтверждающие теоретические выкладки.

Литература

1. General Data Protection Regulation - GDPR. URL: gdpr-info.eu/. Date accessed: 15.01.2023

2. Naik N. and Jenkins P., Your Identity is Yours: Take Back Control of Your Identity Using GDPR Compatible Self-Sovereign Identity, 2020 7th International Conference on Behavioural and Social Computing (BESC), Bournemouth, 2020, United Kingdom, pp. 1-6, doi: 10.1109/BESC51023.2020.9348298.

3. Naik N. and Jenkins P., Self-Sovereign Identity Specifications: Govern your identity through your digital wallet using blockchain technology, in 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud 2020). IEEE, 2020, Oxford, UK, pp. 90-95, doi: 10.1109/MobileCloud48802.2020.00021.

4. Naik N. and Jenkins P., uPort Open-Source Identity Management System: An Assessment of Self-Sovereign Identity and User-Centric Data Platform Built on Blockchain, 2020 IEEE International Symposium on Systems Engineering (ISSE), Vienna, Austria, 2020, pp. 1-7, doi: 10.1109/ISSE49799.2020.9272223.

5. Jing S., Zheng X. and Chen Z., Review and Investigation of Merkle Tree's Technical Principles and Related Application Fields, 2021 International Conference on Artificial Intelligence, Big Data and Algorithms (CAIBDA), Xi'an, China, 2021, pp. 86-90, doi: 10.1109/CAIBDA53561.2021.00026.

6. Source Code of Bitcoin Network, URL: github.com/bitcoin/bitcoin, дата обращения: 20.01.2023.

7. Приказчиков, Д. Е., Малахов С. В. Механизмы консенсуса proof of work и proof of stake на примере платформы Ethereum, Инновации. Наука. Образование. – 2021. – № 34. – С. 1093-1098.

8. Шенявский Н. И., Валутина А. Д., Третьяк М. А., Лопаткин А.С., Пиневич Е.В. Сравнительный анализ основных алгоритмов достижения согласованности - Proof of Work и Proof of Stake, Модернизация образования в условиях технологических и цифровых нововведений: теория и практика: материалы XL Всероссийской научно-практической конференции, Ростов-на-Дону, 12 ноября 2021 года. Том Часть 2. – Ростов-на-Дону: Южный университет (ИУБиП), 2021. – С. 106-108.

9. Nguyen C. T., Hoang D. T., Nguyen D. N., Niyato D., Nguyen H. T. and Dutkiewicz E., Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities, 2019, in IEEE Access, vol. 7, pp. 85727-85745, doi: 10.1109/ACCESS.2019.2925010.

10. Ethereum Proof Of Stake. URL: ethereum.org/en/developers/docs/consensus-mechanisms/pos/, дата обращения: 01.02.2023

11. Ding, Yepeng & Sato, Hiroyuki. (2022). Self-Sovereign Identity as a Service: Architecture in Practice. 10.48550/arXiv.2205.08314.

12. Bin Cao, Zhenghui Zhang, Daquan Feng, Shengli Zhang, Lei Zhang, Mugen Peng, Yun Li, Performance analysis and comparison of PoW, PoS and DAG based blockchains, Digital Communications and Networks, Volume 6, Issue 4, 2020, Pp. 480-485, URL: doi.org/10.1016/j.dcan.2019.12.001.

13. Акутин, А. С., Бровко А.В. Система суверенной личности на основе распределенного реестра данных, Вестник Саратовского государственного технического университета. – 2021. – № 4(91). – С. 5-12.

References

1. General Data Protection Regulation. GDPR. URL: gdpr-info.eu/

2. Naik N. and Jenkins P., 2020 7th International Conference on Behavioural and Social Computing (BESC), Bournemouth, United Kingdom, 2020, pp. 1-6, doi: 10.1109/BESC51023.2020.9348298.

3. Naik N. and Jenkins P., in 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud 2020). IEEE, 2020, Oxford, UK, 2020, pp. 90-95, doi: 10.1109/MobileCloud48802.2020.00021.

4. Naik N. and Jenkins P., 2020 IEEE International Symposium on Systems Engineering (ISSE), Vienna, Austria, 2020, pp. 1-7, doi: 10.1109/ISSE49799.2020.9272223.

5. Jing S., Zheng X. and Chen Z., 2021 International Conference on Artificial Intelligence, Big Data and Algorithms (CAIBDA), Xi'an, China, 2021, pp. 86-90, doi: 10.1109/CAIBDA53561.2021.00026.

6. Source Code of Bitcoin Network. URL: github.com/bitcoin/bitcoin.

7. Prikazchikov, D. E., Malaxov S. V., Innovacii. Nauka. Obrazovanie. 2021. № 34. pp. 1093-1098.

8. Shenyavskij N. I., Valutina A. D., Tret`yak M. A., Lopatkin A.S., Pinevich E.V. materials from XL Vserossijskoj nauchno-prakticheskoj konferencii, Rostov-na-Donu, 2021, Tom Chast` 2. Rostov-na-Donu: Yuzhny`j universitet (IUBiP), 2021. P. 106-108. EDN PPPDHT.

9. Nguyen C. T., Hoang D. T., Nguyen D. N., Niyato D., Nguyen H. T. and Dutkiewicz E., Applications and Opportunities, in IEEE Access, vol. 7, pp. 85727-85745, 2019, doi: 10.1109/ACCESS.2019.2925010.

10. Ethereum Proof Of Stake. URL: ethereum.org/en/developers/docs/consensus-mechanisms/pos/

11. Ding, Yepeng & Sato, Hiroyuki. (2022). 10.48550/arXiv.2205.08314.

12. Bin Cao, Zhenghui Zhang, Daquan Feng, Shengli Zhang, Lei Zhang, Mugen Peng, Yun Li, Digital Communications and Networks, Volume 6, Issue 4, 2020, Pp. 480-485. URL: doi.org/10.1016/j.dcan.2019.12.001.

13. Akutin, A. S., Brovko A.V., Vestnik Saratovskogo gosudarstvennogo texnicheskogo universiteta. 2021., № 4(91)., pp. 5-12.