Научная статья
УДК 34:004:347.211:004.8
EDN: https://elibrary.ru/mloxmi
DOI: https://doi.org/10.21202/jdtl.2024.29

Новый подход к преодолению конфликта между «правом на забвение» и технологией блокчейн

Фабио Северино

Traent SRL, Пиза, Италия

Людовика Спозини ✉

Школа перспективных исследований Сант'Анна, Пиза, Италия

Ключевые слова

блокчейн гибридный,
блокчейн публичный,
блокчейн частный,
Европейский союз,
законодательство
защита персональных данных,
Общий регламент по защите данных,
право,
право на забвение,
цифровые технологии

Аннотация

Цель: в статье рассматриваются проблемы, связанные с конфликтом между технологией блокчейн и «правом на забвение», предусмотренным европейской системой защиты данных.

Методы: в первом разделе кратко описаны эволюция технологии блокчейн, а также наиболее актуальные проблемы, возникающие между традиционными моделями блокчейна и законодательством Европейского союза. Среди последних проанализирован конкретный вопрос конфликта между природой традиционных блокчейнов (как частных, так и публичных моделей), как правило, неизменяемых, и правом индивида требовать удаления или изменения своих персональных данных. В этом разделе отмечается важность задачи по защите персональных данных, которая всегда была одной из главных для наднациональных законодателей. Приводится анализ правового регулирования защиты данных и соответствующей практики Европейского суда по правам человека. Поднимается проблема выражения свободного самоопределения личности в виде контроля над управлением персональными данными в Интернете. Второй раздел посвящен изучению возможных путей решения сложившегося противоречия, позволяющих сделать систему распределенных реестров совместимой с европейским законодательством о защите данных. Сделан акцент на модели, предложенной компанией Traent, гарантирующей право на удаление и изменение данных. Анализируются возможности данной модели по разрешению указанного противоречия.

✉ Контактное лицо

Результаты: рассмотрены особенности новой модели и ее возможности по стратегическому использованию преимуществ публичных и частных блокчейнов. Показано, что данная модель гарантирует не только достоверность и подлинность цепочки, по которой была проведена транзакция, но и, что особенно важно, изменение и полное удаление персональных данных пользователя. Это инновационное решение потенциально дает возможность справиться с противоречием между требованиями конфиденциальности данных и развитием блокчейна в европейском контексте.

Научная новизна: компании Traent удалось реализовать «гибридную» модель, которая включает в себя как публичные, так и частные компоненты блокчейна, что позволяет достичь эффективного соответствия нормам Европейского союза в отношении защиты и конфиденциальности данных.

Практическая значимость: полученные выводы и предложения могут учитываться при совершенствовании соответствия блокчейн-технологий принципам Общего регламента Европейского союза по защите персональных данных.

Для цитирования

Северино, Ф., Спозини, Л. (2024). Новый подход к преодолению конфликта между «правом на забвение» и технологией блокчейн. *Journal of Digital Technologies and Law*, *2*(3), 565–584. https://doi.org/10.21202/jdtl.2024.29

Содержание

Введение

2008 г. стал поворотным для так называемой эры цифровой революции. Именно тогда была опубликована статья Сатоши Накамото «Биткоин: одноранговая система электронных денег»[1]. Это произошло в рамках движения «киберпанк», выступавшего

[1] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://clck.ru/3EGDkg

против вызванных новыми технологиями ограничений индивидуальных свобод, и в частности, права на неприкосновенность частной жизни. Для достижения этой цели биткоин представлялся полезным инструментом: это электронная валюта, широко использующая криптографические технологии и позволяющая создавать безопасные и неопровергаемые системы обмена товарами, услугами и, прежде всего, информацией.

Накамото предложил создать коммуникационный протокол, т. е. неизменяемый реестр, организованный в отдельные блоки, каждый из которых содержит одну или несколько транзакций. Они соединяются вместе, образуя цепочку, отсюда и название «блокчейн». Каждый блок имеет «заголовок», в котором содержится хэш – ряд букв и цифр, кодирующий все транзакции, записанные в этом блоке, – а также отметка времени и хэш предыдущего блока.

При этом используются различные технологии, включая: i) шифрование с асимметричным ключом, позволяющее проверить источник сообщений, а также их целостность; ii) одноранговую систему, преимущество которой заключается в отсутствии необходимости в центральном органе для подтверждения транзакций; iii) «доказательство работы» – механизм формирования консенсуса, основанный на использовании вычислительных ресурсов для решения математической задачи. Иначе говоря, узел, которому первому удается распространить правильное решение среди остальных участников сети, получает вознаграждение за оказанную услугу. В то же время система обеспечивает корректность этого результата именно тем, что для его получения задействовано большое количество ресурсов[2].

В основе данной технологии лежит сеть компьютеров, которые обмениваются между собой распределенным реестром, содержащим копии всех транзакций, совершенных в цепочке. Таким образом, можно гарантировать, с одной стороны, безопасность системы регистрации, поскольку переписать все блоки было бы очень сложно; с другой – ее прозрачность, поскольку каждый раз, когда совершается новая транзакция, она записывается в каждую «копию» распределенного реестра. Это означает, что каждый участник может проверять транзакции и иметь доступ к данным без необходимости наличия централизованной высшей инстанции. Вместо этого система перераспределяет полномочия по проверке между пользователями в практически равных долях, создавая эффективную, прозрачную и, прежде всего, более демократичную систему[3]. Эта технология, изначально созданная для обмена криптовалют, благодаря

---

2 Следует отметить, что это лишь один из многих существующих механизмов консенсуса, включая: i) так называемое доказательство владения (Proof of Stake, PoS), согласно которому возможность подтверждения транзакций прямо пропорциональна количеству активов, которыми обладает узел; ii) делегированное доказательство владения (Delegated Proof of Stake), основанное на своего рода голосовании, при котором каждый пользователь, обладающий активами в системе, может делегировать подтверждение транзакции другому; iii) консенсус на основе депозита (Deposit-based consensus), при котором для добавления блока в блокчейн необходимо сначала внести обязательный депозит; iv) доказательство существования (Proof of Existence), при котором валидацию могут осуществлять только те, кто имеет определенные полномочия или документы; v) доказательство полномочий (Proof of Authority, PoA), при котором полномочия на валидацию транзакций предоставляются исключительно на основе идентификации самого узла. Подробное объяснение каждого механизма см. (Sarzana & Nicotra, 2018).

3 European Parliament. (2017). How blockchain technology could change our lives – In-depth analysis, где говорится: «Блокчейн частично забирает контроль над повседневным взаимодействием с технологиями у центральных элит, перераспределяя его между пользователями. При этом системы становятся более прозрачными и, возможно, более демократичными» (4). См. также (Lacity & Treiblmaier, 2022).

своему потенциалу сразу же распространилась далеко за пределы этой области (Sarzana & Nicotra, 2018; Rajasekaran et al., 2022; Belotti et al., 2019; Michael et al., 2018; Ammous, 2016)[4] и теперь находит применение от сектора финансовых услуг, здравоохранения, управления цепочками поставок, так называемого электронного голосования[5] до цифровых товаров (например, NFT) и паспортов товаров.

В 2015 г. произошел переход к так называемым технологиям второго поколения. Это выразилось в разработке Ethereum – первого программируемого блокчейна, способствовавшего появлению смарт-контрактов и развитию децентрализованных приложений на блокчейне. Более того, достоинства этой технологии вскоре были признаны и европейским законодателем. Было заявлено, что ее использование может ускорить процесс согласования и исполнения сделок, что дает значительные преимущества для развития внутреннего рынка[6]. Однако отмечалось также, что законодательство Европейского союза, сформировавшееся до появления блокчейна, не может справиться с возможными рисками и опасностями, которые блокчейн представляет для основных прав, и прежде всего, для защиты персональных данных[7].

1. Определение, функционирование и основные особенности технологии блокчейна

С 2008 г. было реализовано несколько блокчейнов, каждый из которых имеет свои отличительные особенности. Из-за этой неоднородности очень трудно (если вообще возможно) дать единое и общее определение этому явлению[8]. Тем не менее можно сделать некоторые общие выводы.

Прежде всего, технология блокчейн является подкатегорией «технологии распределенных реестров» (Distributed Ledgers Technology, DLT), т. е. особых типов баз данных, в которых данные записываются, совместно используются и синхронизируются в распределенной сети компьютеров. Данные могут иметь любую меновую стоимость, поддающуюся экономической оценке; например, это могут быть деньги, контракты, истории болезней, сделки купли-продажи товаров и услуг, свидетельства о рождении или браке. Однако следует отметить, что DLT отличаются от блокчейна способом записи и проверки информации.

---

4 Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. https://clck.ru/3EGEp4

5 Подробный анализ этих вопросов см. (European Parliament. (2017). How blockchain technology could change our lives – In-depth analysis; Gupta et al., 2023; Mccorry et al., 2021).

6 European Parliament. (2022). Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU (Text with EEA relevance).

7 Там же.

8 (Walch, 2016). Стоит отметить, что чрезвычайное разнообразие блокчейна не позволяет выработать общепринятое (и приемлемое) инклюзивное определение всех типов платформ, существующих на рынке в настоящее время (и тех, которые появятся в будущем). Однако если появится такое определение этого явления, которое позволит очертить его границы и, таким образом, рассматривать его в едином ключе, то оно неизбежно будет отличаться излишней жесткостью, которая плохо сочетается с технологическими изменениями. Поэтому предпочтительно, как это уже было отмечено в авторитетных источниках в отношении определения цифровой платформы, использовать функциональный подход для каждой конкретной ситуации. По этому вопросу см. (Bertolini et al., 2021).

Как уже говорилось, это распределенные базы данных, поскольку они работают в сети из нескольких узлов, обычно установленных на одном компьютере (технически – на сервере). При выполнении транзакции она передается в сеть, которая проверяет ее в соответствии с алгоритмом консенсуса (Sarzana & Nicotra, 2018). Таким образом, каждый блок в цепочке, формирующей реестр, неизменяемо связан с предыдущим и последующим блоками. Другими словами, после добавления блока он уже не может быть изменен без внесения изменений в последующую часть цепочки. Это гарантирует целостность реестра, поскольку для переписывания последующих блоков потребовалось бы одновременно переписать весь реестр, а это невыполнимая операция из-за стоимости и требуемой вычислительной мощности. Затем все данные становятся общедоступны для каждого узла в сети и непрерывно обновляются и синхронизируются.

1.1. Единая технология, различные классификации

В обиходе термин «блокчейн» используется для общего обозначения технологии, основанной на распределенном реестре. На самом деле в эту категорию входят различные типы блокчейнов, каждый из которых имеет свои характеристики и особенности.

Существуют так называемые публичные блокчейны, основополагающим свойством которых является их «децентрализованность». Во-первых, они, как правило, являются «безразрешительными», т. е. пользователи могут выполнять любые операции, в том числе читать существующие и предлагать новые блоки, а также подтверждать транзакции. Иными словами, таким блокчейнам (примером служит платформа Bitcoin) не требуется центральный орган, который выступал бы в качестве посредника или подтверждал транзакции, происходящие в сети. Вместо этого они используют одноранговый механизм, т. е. напрямую соединяют пользователей, которые одновременно становятся активными субъектами для подтверждения транзакций и пассивными, поскольку владеют всей информацией. Как мы уже упоминали выше (Sarzana & Nicotra, 2018), это система, основанная на так называемом механизме консенсуса, поскольку все участники обязаны проверять и создавать транзакции, следуя определенным правилам, которые уже закодированы в программном обеспечении блокчейна. Например, одним из наиболее широко используемых алгоритмов консенсуса является алгоритм «доказательство работы» (Proof of Work, PoW), который опирается на вычислительную мощность компьютеров (называемых «майнерами») для быстрого решения математических задач, которые становятся все более сложными после каждой подтвержденной транзакции. Кроме того, у каждого участника хранится копия реестра. Таким образом, каждый может участвовать в работе сети, а все данные доступны в любое время и в любом месте.

Такой одноранговый механизм делает систему гораздо более устойчивой к возможным атакам, поскольку для этого необходимо поразить большинство узлов, распределенных в сети (Aponte-Novoa et al., 2021). Фактически каждое изменение быстро становится видимым для всех участников, а криптографические подписи гарантируют целостность и аутентичность транзакций (это называется «устойчивостью к взлому» (Austin & Di Troia, 2022)).

Поэтому за каждую правильно подтвержденную транзакцию предусмотрены различные системы вознаграждения, а также действуют протоколы, делающие неправомерное поведение крайне затруднительным.

Из этих кратких рассуждений уже можно понять преимущества и недостатки открытого блокчейна этого типа. Децентрализованная (и, следовательно, распределенная) система обеспечивает как целостность транзакций, так и большую безопасность, поскольку ее сложнее атаковать. Кроме того, транзакции хранятся неограниченное время, что гарантирует верифицируемость всей цепочки. Наконец, они являются публичными и, следовательно, общедоступными, поскольку отсутствует централизованный контроль со стороны какого-либо органа.

С другой стороны, публичные блокчейны, как правило, очень медленно обрабатывают транзакции и, значит, плохо подходят для обработки больших объемов информации. Это связано с тем, что у них есть серьезная проблема масштабируемости, т. е. с увеличением количества узлов в сети скорость выполнения и обработки транзакций снижается[9]. Не говоря уже о воздействии на окружающую среду, которое оказывают такие модели[10].

Существуют и «частные» блокчейны, доступ к которым имеют только авторизованные пользователи. Соответственно, персональные (и другие) данные участников сети распространяются только внутри нее. В частности, речь идет о пользователях, чья личность хорошо известна, поскольку для того, чтобы стать узлом, необходимо выполнить ряд требований и получить одобрение центрального администратора. Кроме того, желающие присоединиться к сети часто должны подписать условия обслуживания, определяющие их права и обязанности. Поэтому очевидно, почему в данном случае не требуются особо строгие механизмы консенсуса: здесь системе не нужно «завоевывать» доверие операторов с помощью дорогостоящих механизмов консенсуса, поскольку каждый узел, будучи легко идентифицируемым и узнаваемым, несет бремя ответственности (Raymond Choo et al., 2020). В системах такого типа проверка транзакций обычно делегируется доверенному подмножеству узлов. Другими словами, если публичный блокчейн в некотором роде можно назвать олицетворением демократии и децентрализации, то в частных реализована парадигма олигархии: не все узлы имеют равное значение.

Такая система, несомненно, имеет ряд технических преимуществ. Во-первых, она гораздо быстрее (поскольку только очень небольшая группа узлов отвечает за проверку и распространение новых блоков), а во-вторых, благодаря возможности ограничить доступ к содержимому блокчейна, она кажется более безопасной с точки зрения конфиденциальности и приватности. Однако именно здесь кроется одна из главных слабостей частных моделей. Если в публичных моделях безопасность технологии обусловлена распределением и децентрализацией реестра, то в частных моделях он не распределяется, а концентрируется в руках одного или нескольких субъектов.

---

[9] Проблемы масштабируемости алгоритма «доказательство работы» обусловлены его конструкцией, которая требует значительных вычислительных мощностей для проверки транзакций и добавления блоков. При подключении большего количества узлов они все равно должны обрабатывать и подтверждать все транзакции независимо от того, что снижает общую пропускную способность. Кроме того, высокое энергопотребление и медленная передача блоков еще больше ограничивают масштабируемость этого алгоритма, что приводит к увеличению времени транзакций и повышению стоимости в периоды пикового спроса. По этому вопросу см. (Gramoli, 2022).

[10] Подробнее о влиянии блокчейна на окружающую среду см. Bitcoin Energy Consumption Index. Digiconomist. https://clck.ru/3EGHgF

Обе описанные категории, в свою очередь, могут быть «разрешительными» или «безразрешительными»[11]. Так, существуют «публичные безразрешительные блокчейны», в которых любой человек может участвовать в механизме консенсуса и предлагать транзакции (это, например, касается таких платформ, как Bitcoin или Ethereum), и «публичные разрешительные блокчейны», которые позволяют всем пользователям видеть журнал транзакций и совершать любые операции, хотя в механизме консенсуса участвует лишь небольшое количество узлов. Ярким примером является Ripple[12].

То же относится и к частным блокчейнам[13], где различают «частные разрешительные блокчейны», которые ограничивают транзакции и возможности отображения реестра только теми узлами, которые участвуют в сети, и оператор платформы сам выбирает, кому разрешить участвовать в механизме консенсуса. Так происходит, например, в случае Rubix[14]. Прямо противоположное происходит в «частных безразрешительных блокчейнах»[15], которые ограничивают круг лиц, которым разрешено совершать транзакции и получать доступ к реестру, но, в отличие от первых, здесь механизм консенсуса открыт для всех.

1.2. Публичный и частный блокчейн… и третий путь

Как публичные, так и частные блокчейны имеют свои преимущества и недостатки. Первые, как мы показали, обладают «универсальной» прозрачностью (поскольку транзакции видны всем участникам сети), надежны (благодаря своей децентрализованной природе они менее подвержены одномоментным отказам системы), децентрализованы, доступны (ими управляет глобально распределенная сеть узлов, что делает их очень устойчивыми) и неизменяемы. Однако они очень медленные, поскольку имеют проблему масштабируемости из-за объема транзакций и необходимости децентрализованного подтверждения; у них очень высокая стоимость транзакций, и они не гарантируют конфиденциальность, поскольку являются публичными. Аналогичным образом, частные блокчейны, безусловно, более эффективны, поскольку они масштабируются и работают быстрее (это объясняется тем, что нет необходимости в децентрализованном подтверждении и, следовательно, транзакции обрабатываются быстрее); они гарантируют конфиденциальность информации, содержащейся в сети, и организаторы сети полностью контролируют управление и правила сети. С другой стороны, частные блокчейны менее прозрачны, централизованы и менее безопасны.

Чтобы решить некоторые из проблем, присущих этим двум моделям, был разработан третий тип блокчейна – «гибридный». Эти модели обладают характеристиками

---

11 Ismail, A. (2020). Permissioned Blockchains for Real World Applications. Lakehead University.

12 Ripple. https://clck.ru/3EGDyK

13 Nascimento, S. et al. (2019). Blockchain Now and Tomorrow: Assessing Multidimensional Impacts of Distributed Ledger Technologies. European Commission. https://clck.ru/3EGDUk

14 Rubix. https://clck.ru/3EGE3L

15 Однако следует отметить, что это очень редкий случай, поскольку частный безразрешительный блокчейн – это некое противоречие, так как «частный» обычно подразумевает ограниченный доступ, а «безразрешительный» – открытый доступ. Однако можно разработать блокчейн с некими гибридными характеристиками.

публичных и частных блокчейнов, но предлагают большую гибкость и адаптируемость к широкому спектру ситуаций использования. Во-первых, они гибкие, поскольку позволяют настраивать степень децентрализации и конфиденциальности в соответствии с конкретными потребностями приложения, для которого они используются. С другой стороны, такие системы более надежны, поскольку, объединяя публичные и частные элементы, можно повысить общую помехоустойчивость сети (Smith, 2020). Кроме того, они совместимы между собой и могут решать проблемы масштабируемости, уравновешивая параметры контроля и децентрализации. Однако сочетание публичных и частных факторов может привести к повышению уровня сложности системы, что, в свою очередь, чревато появлением новых уязвимостей в системе безопасности. Наконец, разработка и внедрение гибридного блокчейна могут потребовать значительных ресурсов и очень высоких затрат.

1.3. Кейс: компания Traent и преимущества гибридного блокчейна

Переход к гибридному блокчейну представляет собой важный момент эволюции этой области, которая отличается особой гибкостью и адаптивностью. С этой целью итальянская компания Traent[16] реализовала гибридную модель блокчейна, способную объединить преимущества (и устранить недостатки) как публичных, так и частных систем[17].

Как уже упоминалось ранее, в публичных блокчейнах каждый узел, участвующий в сети, имеет копию реестра, поэтому каждая копия содержит все транзакции и криптографические доказательства, связанные с каждым блоком в цепи. По этой причине публичный блокчейн более безопасен, поскольку для изменения транзакции потребуется, чтобы все узлы, которых потенциально бесконечное множество, изменили цепочку («устойчивость к ветвлению»[18]). Однако именно потому, что модифицировать цепочку и переписать ее очень сложно, данные в ней нельзя изменить или удалить после опубликования.

С другой стороны, частные блокчейны пытаются решить именно эту проблему: поскольку они распространяются среди ограниченного числа участников, можно ограничить обмен данными. Критическая важность этого механизма обусловлена тем, что пользователи, которые по определению не могут быть беспристрастными, также ответственны за подтверждение транзакций, происходящих на платформе. Это означает, что они могут легко изменить записи в цепочке, поскольку нет третьей стороны с функцией независимого контроля. У стороннего пользователя нет возможности проверить, была ли изменена цепочка.

---

16 Traent. https://clck.ru/3EGJHN

17 Следует отметить, что описание технического функционирования платформы выходит за рамки данного обсуждения, поэтому мы отсылаем к работе (Pelosi et al., 2023). Однако представляется целесообразным вкратце описать принцип работы системы Traent, чтобы читатель мог лучше разобраться в проблемах «права на забвение» и блокчейна.

18 Устойчивость к ветвлению – это способность сети блокчейн противостоять и восстанавливаться после хардфорка, т. е. необратимого расхождения ветвей блокчейна, вызванного конфликтующими правилами. Хардфорки возникают в результате спорных обновлений сети и могут привести к созданию новой криптовалюты. См. (Golden et al., 2020).

Блокчейн, предложенный компанией Traent, напротив, добивается «внешней» (или даже «публичной») проверяемости именно за счет использования гибридной модели. В частности, компания предоставляет заинтересованным пользователям частный блокчейн для совершения любой транзакции, которая материализуется в частном реестре в виде блока вместе с криптографическим доказательством. Впоследствии это доказательство публикуется на внешнем публичном блокчейне с помощью системного компонента под названием Notary (Pelosi et al., 2023). Таким образом, криптографические доказательства, связанные с отдельными блоками, записанными в (частном) реестре, публикуются в (публичном) блокчейне. Таким образом, пользователь может быть уверен, что транзакции не были изменены другими пользователями. Отсутствие ветвлений в цепочке проверяется на внешнем блокчейне благодаря внешнему криптографическому доказательству.

2. Конфликт между технологией блокчейн и «правом на забвение» в контексте европейского законодательства в области защиты данных. Решение компании Traent

Признание «права на забвение» в качестве фундаментального элемента защиты личной идентичности и свобод человека – недавнее достижение современного общества, основанного на модели платформенной экономики (Xue et al., 2020; Cohen, 2017; Kenney & Zysman, 2016; Stark & Pais, 2020; Acs et al., 2021). Защита персональных данных всегда была главной задачей наднациональных законодателей; она признана в Хартии основных прав Европейского союза в качестве автономного и независимого права[19] на частную и семейную жизнь[20]. Чтобы эффективно применять этот принцип и в то же время обеспечить свободное перемещение и защиту данных в рамках Евросоюза, Комиссия представила в 2012 г. пакет документов, направленных на гармонизацию законодательства в этой области между государствами-членами.

В этом отношении существенный вклад внесла судебная практика Суда Европейского союза (далее – CEC), и в частности, известное дело Google Spain[21]. Дело касалось гражданина Испании, который обратился к оператору интернет-сайта и компании Google как поисковой системе, чтобы добиться удаления своих данных, опубликованных за несколько лет до этого в одной из национальных газет. В частности, истец заявил, что данные больше не являются актуальными, и требовал права на то, чтобы поисковая система не перенаправляла пользователей на страницу, где сообщалась недостоверная информация. В своем решении суд изложил ряд основных принципов эффективного осуществления права пользователей на удаление своих персональных данных в Интернете. Среди различных вопросов, затронутых в этом решении, суд признал право пользователя требовать,

19 Хартия Европейского союза об основных правах, OJ C 326, 26.10.2012 (cc. 391–407), Ст. 8.

20 Там же, Ст. 7.

21 CJEU, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12, 13 May 2014, ECLI:EU:C:2014:317.

чтобы определенный вредный контент больше не был доступен в сети и, соответственно, не индексировался в результатах поиска платформы. Это объясняется тем, что, по мнению CEC, основные права, предусмотренные ст. 7 и 8 Ниццкого договора, должны превалировать над экономическими интересами провайдера, а также общества.

Несмотря на то, что наднациональный суд совершенно однозначно подтверждает высокую значимость причин, по которым пользователь претендует на право удаления информации, этого нельзя сказать о практике Европейского суда по правам человека. В качестве примера можно привести дело Węgrzynowski and Smolczewski v. Poland, где выводы были совершенно иными[22]. В этом решении ЕСПЧ не признает право пользователя на удаление онлайн-информации, а пытается найти баланс между свободой выражения мнения в соответствии со статьей 10 ЕКПЧ и «правом на забвение». Иными словами, суд счел полное удаление контента несоразмерным, а наиболее подходящим средством защиты было признано требование к онлайн-издателю опубликовать дополнительные разъяснения к статье, т. е. предоставить обновленную информацию по теме.

Впоследствии, в 2016 г., Европейский союз принял Общий регламент по защите данных 2016/679 (General Data Protection Regulation, далее – GDPR)[23], в котором в ст. 17 «Право на удаление (“право на забвение”)» наконец было четко указано, что «субъект данных имеет право требовать от контролера незамедлительного удаления относящихся к нему персональных данных, контролер должен незамедлительно удалить персональные данные»[24].

Таким образом, это положение признает два различных права: с одной стороны, право на «удаление данных», которое позволяет субъекту данных требовать удаления данных о нем, исходя из того, что по истечении определенного периода времени они больше не представляют интереса и не отражают его личность. С другой стороны, это положение также признает «право на забвение» в строгом смысле, которое шире

---

22 CEDU, Węgrzynowski and Smolczewski v. Poland, Application No. 33846/07, 16 July 2013. https://clck.ru/3EGJgf

23 European Parliament and Council. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

24 Далее в документе определены условия, необходимые для реализации этого права пользователем: (a) персональные данные больше не требуются для целей, для которых они были получены или обрабатывались в иных случаях; (b) субъект данных отзывает свое согласие, на основании которого? согласно пункту (a) ст. 6(1) или пункту (a) ст. 9(2), проводилась обработка, и если отсутствует иное юридическое основание для обработки; (c) субъект данных возражает против обработки согласно ст. 21(1), и отсутствуют имеющее преимущественную юридическую силу законные основания для обработки, или субъект данных возражает против обработки согласно ст. 21(2); (d) персональные данные обрабатывались незаконно; (e) персональные данные должны быть уничтожены в целях соблюдения юридической обязанности согласно законодательству Союза или государства – члена ЕС, под действие которого подпадает контролер; (f) персональные данные собирались в отношении предоставления услуг информационного общества согласно ст. 8(1). Кроме того, ст. 16 предусматривает право на исправление данных. Подробное обсуждение права на забвение после принятия GDPR см. (Alessi, 2017; Kocharyan et al., 2021; Mantelero, 2013; Politou et al., 2018; Finocchiaro, 2010; Peguera, 2019).

первого и требует от контролера удалить не только всю информацию, касающуюся субъекта данных, но и любую ссылку, копию или точное повторение указанных данных. Другими словами, предполагается, что пользователь должен иметь более широкий контроль над управлением своими данными в Интернете, что является выражением свободного самоопределения личности.

2.1. Несовместимость между «правом на забвение» и технологией блокчейна

Фундаментальной характеристикой блокчейна является его неизменяемость, что, однако, полностью противоречит статье 17 GDPR, которая позволяет пользователям в любое время потребовать и получить изменение или полное удаление своих данных. Это справедливо как для публичных, так и для частных моделей блокчейна. Первые фактически чрезвычайно безопасны, поскольку используют распределенную систему, в которой каждый участник сети имеет копию реестра. Однако это преимущество имеет тот недостаток, что изменить или удалить данные после их внесения в цепочку невозможно, так как информация должна быть удалена с каждого узла (действует так называемый принцип неизменности публичного блокчейна). С другой стороны, частные блокчейны пытаются решить эту проблему, позволяя пользователям выбирать, какие данные публиковать, а какие нет (и с кем ими делиться), однако за счет того, что система не является полностью безопасной. То же самое можно сказать и о простом изменении или исправлении данных, поскольку каждый блок в блокчейне содержит информацию о данных в предыдущем блоке. Это означает, что, если попытаться изменить информацию в одном блоке цепи, последующие блоки не пройдут верификацию.

Было разработано несколько альтернативных решений, чтобы сделать систему совместимой с европейским законодательством о защите данных, поскольку в ст. 17 не указано, как конкретно должно быть достигнуто «удаление» данных. Одни считали, что достаточно простого обезличивания данных, другие предлагали «вывести данные из употребления», т. е. обеспечить, чтобы контролер данных больше не мог использовать информацию в целях принятия решений и передать ее третьей стороне, принимал технические меры для защиты данных и, наконец, был обязан удалить данные, когда это возможно. Еще один вариант – сделать данные полностью недоступными, уничтожив закрытый ключ, соответствующий открытому ключу, которым владеет каждый пользователь сети. В этом отношении даже CEC не совсем ясно толкует норму GDPR, но, видимо, признает, что стирание означает полное уничтожение данных. В частности, в деле Peter Nowak v Data Protection Commissioner за кандидатом на письменном экзамене было признано «право потребовать контролера данных обеспечить стирание, т. е. уничтожение, его экзаменационных ответов и комментариев экзаменатора к ним через определенный период времени»[25]. По этому поводу Европейский центр парламентских исследований (European Parliamentary Research Service, EPRS)[26] также заявил, что

[25] CJEU, Peter Nowak v Data Protection Commissioner, Case C-434/16, 20 December 2017, ECLI:EU:C:2017:994.

[26] Service EPR. (2019). Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?

«неясно, можно ли рассматривать это как общее утверждение, что стирание данных всегда равносильно уничтожению, тем более что в рассматриваемом деле право на стирание не рассматривалось напрямую. Таким образом, это заявление можно объяснить конкретным контекстом и тем фактом, что прямое уничтожение копии экзаменационных записей может быть наиболее простым способом уничтожения (хотя еще одним очевидным вариантом является вымарывание соответствующей информации)»[27].

2.2. Модель, разработанная компанией Traent, гарантирующая право на удаление и изменение данных

Компания Traent предлагает интересное решение, гарантирующее соблюдение права на забвение, а именно гибридный блокчейн. Эта модель предусматривает запись в блок (частного) реестра не всех данных, а лишь «ссылки»[28] на ту часть цепи, где хранятся данные. Кроме того, в этот же блок вставляется криптографическое доказательство («дайджест»). Таким образом, благодаря ссылке, записанной в (частной) цепочке, заинтересованный пользователь может получить доступ к полным внешним данным и с помощью дайджеста проверить, что они не были изменены.

Этот двойной механизм не только делает систему более безопасной, поскольку позволяет удостовериться в подлинности информации, содержащейся в блокчейне, но и позволяет пользователям удалять введенные данные: поскольку они находятся за пределами частного блокчейна, их можно удалить, не изменяя цепочку. Таким образом, верификация блокчейна остается действительной, поскольку блоки реестра фактически никогда не изменяются. Однако, поскольку дайджест связан с этими внешними данными (которых больше не существует, так как они были удалены), он перестает работать. В этот момент гибридная модель, разработанная компанией Traent, создает новый блок, вставляемый в частный реестр, в котором данные (к которым ведет ссылка и криптографическое доказательство), содержащиеся в предыдущем блоке, считаются удаленными. Благодаря этой системе пользователь может проверить, что цепочка не была изменена мошенническим путем, и в то же время данные являются подлинными, поскольку из следующего блока ясно, что была произведена операция по удалению данных.

Уже из этих кратких рассуждений ясно, что решение, предложенное компанией Traent, безусловно, в наибольшей степени соответствует ст. 17 GDPR, поскольку позволяет не только полностью удалять данные, но также и изменять их. Таким образом, удается полностью реализовать как европейский регламент, так и интерпретацию, которую, как представляется, дал ему CEC.

---

27 Там же.

28 Это может быть, например, URL.

Заключение

Европейский парламент недавно принял Закон об искусственном интеллекте (Artificial Intelligence Act, AIA)[29], призванный повысить доверие к системам искусственного интеллекта и снизить их риски. Для этого закон запрещает или строго ограничивает использование тех систем, которые представляют неприемлемый риск для безопасности, здоровья, достоинства и независимости человека. Вместе с тем предпринимаются усилия по поддержке инноваций и развитию все более совершенных технологий для использования их полного потенциала на внутреннем рынке[30].

Несмотря на принятие этого закона, вопрос об ответственности систем искусственного интеллекта продолжает волновать экспертов в этой области. В основном это связано с отсутствием эффективных технических решений, позволяющих полностью объяснить причины, побудившие алгоритм выдать тот или иной результат, так что нередко можно услышать о проблеме «черного ящика» (Springer et al., 2017; Veale & Zuiderveen Borgesius). Таким образом, блокчейн может стать ценным инструментом для достижения цели «надежного ИИ»[31]. Во-первых, он обеспечивает прозрачность алгоритмов, поскольку реестр и записи транзакций хранятся безопасно, децентрализованно и доступны всем участникам сети. Кроме того, это гарантирует неизменность результатов: реестр состоит из множества блоков, каждый из которых содержит серию транзакций и данных и защищен криптографической ссылкой на предыдущий блок. Таким образом, даже самое незначительное изменение одного из блоков делает недействительной всю цепочку.

В заключение можно сказать, что на сегодняшний день блокчейн представляется наиболее подходящим, а возможно, и единственным решением, отвечающим требованиям существующего европейского законодательства в области защиты данных и систем искусственного интеллекта. Однако эта технология все еще содержит ряд проблем, требующих решения, среди которых особенно актуальной является гарантия права пользователя на удаление и изменение своей информации. В этом смысле гибридная модель, реализованная компанией Traent, может стать особенно эффективной альтернативой[32], как было кратко продемонстрировано в данной статье. Таким образом, становится возможным полностью использовать потенциал блокчейна для разработки объяснимых алгоритмов и систем искусственного интеллекта, а также устранить или, по крайней мере, снизить любые сомнения в совместимости блокчейна с Общим регламентом Европейского союза по защите персональных данных.

---

29 European Commission. (2021). Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

30 Там же.

31 В Предложении Комиссии по Регламенту Европейского парламента и Совета, устанавливающем гармонизированные правила в области искусственного интеллекта (Artificial Intelligence Act), говорится: «Данное предложение направлено на реализацию второй цели по развитию экосистемы доверия путем создания правовой базы для надежного искусственного интеллекта. Предложение основано на ценностях ЕС и основных правах человека и направлено на то, чтобы дать людям и другим пользователям уверенность в принятии решений на основе ИИ, а также стимулировать предприятия к их разработке» (1). См. также (Nassar et al., 2019).

32 Для более детального ознакомления с технологией Traent и конкретными примерами преимуществ, которые она может дать, см.: Traent. https://clck.ru/3EGKux

Список литературы

Acs, Z. J., Song, A. K., Szerb, L., Andretsch, D. B., & Komlósi, E. (2021). The evolution of the global digital platform economy: 1971–2021. *Small Business Economics*, *57*, 1629–1659. https://doi.org/10.1007/s11187-021-00561-x

Alessi, S. (2017). Eternal sunshine: The right to be forgotten in the European Union after the 2016 General Data Protection Regulation. *Emory International Law Review*, *32*(1), 145.

Ammous, S. (2016). *Blockchain technology: What is it good for?* http://dx.doi.org/10.2139/ssrn.2832751

Aponte-Novoa, F. A., Orozco, A. L. S., Villanueva-Polanco, R., & Wightman, P. (2021). The 51% Attack on Blockchains: A Mining Behavior Study. *IEEE Access*, *9*, 140549–140564. https://doi.org/10.1109/ACCESS.2021.3119291

Austin, T. H., & Di Troia, F. (2022). A Blockchain-Based Tamper-Resistant Logging Framework. In L. Bathen, G. Saldamli, X. Sun, T. H. Austin, & A. J. Nelson (Eds.), *Silicon Valley Cybersecurity Conference. SVCC 2022. Communications in Computer and Information Science* (vol. 1683, pp. 90–104). Springer, Cham. https://doi.org/10.1007/978-3-031-24049-2_6

Belotti, M., Božić, N., Pujolle, G., & Secci, S. (2019). A Vademecum on Blockchain Technologies: When, Which, and How. *IEEE Communications Surveys & Tutorials*, *21*(4), 3796–3838. https://doi.org/10.1109/comst.2019.2928178

Bertolini, A., Episcopo, F., & Cherciu, N.-A. (2021). *Liability of online platforms*. European Parliamentary Research Service (EPRS).

Cohen, J. E. (2017). Law for the platform economy. *UC Davis Law Review*, *51*, 133–204.

Finocchiaro, G. (2010). La memoria della rete e il diritto all'oblio. *Il Diritto Dell'informazione e Dell'informatica*, *3*, 391–404. (In Italian).

Golden, E. J., Najahi, J. J. V., & Jhanjhi, N. Z. (2020). *Blockchain Technology: Fundamentals, Applications, and Case Studies*. Taylor & Francis Ltd. https://doi.org/10.1201/9781003004998

Gramoli, V. (2022). *Blockchain Scalability and its Foundations in Distributed Systems*. Springer Cham. https://doi.org/10.1007/978-3-031-12578-2

Gupta, S., Gupta, A., Pandya, I. Y., Bhatt, A., & Mehta, K. (2023). End to end secure e-voting using blockchain & quantum key distribution. *Materials Today: Proceedings*, *80*, 3363–3370. https://doi.org/10.1016/j.matpr.2021.07.254

Kenney, M., & Zysman, J. (2016). The rise of the platform economy. *Issues in Science and Technology*, *32*(3), 61–69.

Kocharyan, H., Vardanyan, L., Hamuľák, O., & Kerikmäe, T. (2021). Critical views on the right to be forgotten after the entry into force of the GDPR: Is it able to effectively ensure our privacy? *International and Comparative Law Review*, *21*(2), 96–115. https://doi.org/10.2478/iclr-2021-0015

Lacity, M. C., & Treiblmaier, H. (Eds.) (2022). *Blockchains and the Token Economy: Theory and Practice (Technology, Work and Globalization)* (1st ed.). Palgrave Macmillan.

Mantelero, A. (2013). The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'. *Computer Law & Security Review*, *29*(3), 229–235.

Mccorry, P., Mehrnezhad, M., Toreini, E., Shahandashti, S. F., & Hao, F. (2021). On Secure E-Voting over Blockchain. *Digital Threats: Research and Practice*, *2*(4), 33. https://doi.org/10.1145/3461461

Michael, J., Cohn, A., & Butcher, J. R. (2018). Blockchain technology and regulatory investigations. *The Journal Litigation*, *1*, 35–44.

Nassar, M., Salah, K., & Svetinovic, D. (2019). Blockchain for explainable and trustworthy artificial intelligence. *WIREs Data Mining and Knowledge Discovery*, *10*(1), e1340. https://doi.org/10.1002/widm.1340

Peguera, M. (2019). The Right to Be Forgotten in the European Union. In G. Frosio (Ed.), *Oxford Handbook of Online Intermediary Liability*. Oxford University Press.

Pelosi, A., Felicioli, C., Canciani, A., & Severino, F. (2023). A Hybrid-DLT Based Trustworthy AI Framework. In *2023 IEEE International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)* (pp. 1–6). https://doi.org/10.1109/wetice57085.2023.10477792

Politou, E., Michota, A., Alepis, E., Pocs, M., & Patsakis, C. (2018). Backups and the right to be forgotten in the GDPR: An uneasy relationship. *Computer Law & Security Review*, *34*, 1247–1257. https://doi.org/10.1016/j.clsr.2018.08.006

Rajasekaran, A. S., Azees, M., & Al-Turjman, F. (2022). A comprehensive survey on blockchain technology. *Sustainable Energy Technologies and Assessments*, *52*, 102039. https://doi.org/10.1016/j.seta.2022.102039

Raymond Choo, K.-K., Dehghantanha, A., & Parizi, R. M. (Eds.) (2020). *Blockchain Cybersecurity, Trust and Privacy (Advances in Information Security* (1st ed.). Springer Cham. https://doi.org/10.1007/978-3-030-38181-3

Sarzana, F., & Nicotra, M. (2018). *Diritto della blockchain, intelligenza artificiale e IoT*. Ipsoa. (In Italian).

Smith, S. S. (2020). *Blockchain, Artificial Intelligence and Financial Services (Future of Business and Finance)*. Springer Cham.

Springer, A., Hollis, V., & Whittaker, S. (2017). Dice in the Black Box: User Experiences with an Inscrutable Algorithm. In *The AAAI 2017 Spring Symposium onDesigning the User Experience of Machine Learning Systems Technical Report SS-17-04* (pp. 427–430).

Stark, D., & Pais, I. (2020). Algorithmic management in the platform economy. *Sociologica*, *14*(3), 47–72. https://doi.org/10.6092/issn.1971-8853/12221

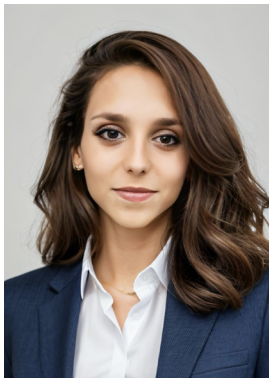
Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International*, *22*(4), 97–112. https://doi.org/10.9785/cri-2021-220402

Walch, A. (2016). The Path of the Blockchain Lexicon (and the Law). *Review of Banking and Financial Law*, *36*, 713–765.

Xue, C., Tian, W., & Zhao, X. (2020). The literature review of platform economy. *Scientific Programming*, *2020*(1), 8877128. https://doi.org/10.1155/2020/8877128

Сведения об авторах

Фабио Северино – технический директор, компания Traent S.r.l.
Адрес: 56127, Италия, г. Пиза, ул. Борго Стретто, 3
E-mail: fabio.severino@traent.com
ORCID ID: https://orcid.org/0000-0002-9538-1218



Людовика Спозини – соискатель степени PhD в области права, Институт права, политики и развития (DIRPOLIS), Школа перспективных исследований Сант'Анна
Адрес: 56127, Италия, г. Пиза, ул. Виа Доменико Вернагалли, 22R
E-mail: ludovica.sposini@santannapisa.it
ORCID ID: https://orcid.org/0000-0003-2188-8996
Google Scholar ID: https://scholar.google.com/citations?user=AVR7_bMAAAAJ

Вклад авторов

Авторы внесли равный вклад в разработку концепции, методологии, валидацию, формальный анализ, проведение исследования, подбор источников, написание и редактирование текста, руководство и управление проектом.

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Благодарность

Авторы выражают благодарность компании Traent SRL за предоставление всей технической документации, касающейся данной технологии, для написания статьи. Кроме того, авторы благодарят за оказанную поддержку Центр передового опыта в области регулирования робототехники и искусственного интеллекта имени Жана Монне (Jean Monnet Centre of Excellence on the Regulation of Robotics and AI, EURA).

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.19.31 / Право на информацию
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 16 июня 2024 г.
Дата одобрения после рецензирования – 2 июля 2024 г.
Дата принятия к опубликованию – 25 сентября 2024 г.
Дата онлайн-размещения – 30 сентября 2024 г.

Research article
UDC 34:004:347.211:004.8
EDN: https://elibrary.ru/mloxmi
DOI: https://doi.org/10.21202/jdtl.2024.29

Overcoming the Friction between the "Right to be Forgotten" and Blockchain Technology through a New Approach

Fabio Severino

Traent SRL, Pisa, Italy

Ludovica Sposini ✉

Sant'Anna School of Advanced Studies, Pisa, Italy

Keywords

digital technologies,
European Union,
General Data Protection Regulation,
Hybrid blockchain,
law,
Legislation,
Personal data protection,
private blockchain,
public blockchain,
right to be forgotten

Abstract

Objective: this paper explores the challenges arising from the conflict between blockchain technology and the "right to be forgotten" as provided by the European data protection framework.

Methods: in the First Section, the author provides a brief description of the evolution of blockchain technology and the most pressing issues between traditional blockchain models and UE's legislations. Among the latter, the author analyzes the specific issue concerning the clash between the traditional blockchains (both private and public models), typically immutable, and the individual's right to cancellation or modification of own personal data. This section emphasizes the importance of personal data protection, which has always been one of the main tasks for supranational legislators. The legal regulation of data protection and the relevant judicial practice of the European Court of Human Rights is analyzed. The author raises the problem of expressing the free self-determination of an individual in the form of controlling their personal data on the Internet. The Second Section of this contribution is dedicated to the study of probable ways to solve the existing incompatibility and to make the distributed ledger system compatible with the European data protection legislation. An emphasis is made on the model provided by "Traent" company, which ensures the right to data cancellation or modification. The capability of this model to solve the said contradiction is analyzed.

✉ Corresponding author

Results: the study delves into the peculiar features of the new model to understand how it strategically utilizes the advantages of public and private blockchains guaranteeing not only the validity and authenticity of the chain where the transaction was performed, but, most importantly, the modification and granular cancellation of client's personal data. This innovative solution offers a potential path forward for navigating the complex intersection of data privacy and blockchain innovation in the European context.

Scientific novelty: Traent has implemented a "hybrid" model blockchain that, incorporating both public and private components, to achieve an effective compliance with the European Union regulations, especially those concerning data protection and privacy.

Practical significance: the obtained conclusions and proposals can be taken into consideration in improving the compliance of blockchain technologies with the European Union General Data Protection Regulation.

For citation

Severino, F., & Sposini, L. (2024). Overcoming the Friction between the "Right to be Forgotten" and Blockchain Technology through a New Approach. *Journal of Digital Technologies and Law, 2*(3), 565–584. https://doi.org/10.21202/jdtl.2024.29

References

Acs, Z. J., Song, A. K., Szerb, L., Andretsch, D. B., & Komlósi, E. (2021). The evolution of the global digital platform economy: 1971–2021. *Small Business Economics*, *57*, 1629–1659. https://doi.org/10.1007/s11187-021-00561-x

Alessi, S. (2017). Eternal sunshine: The right to be forgotten in the European Union after the 2016 General Data Protection Regulation. *Emory International Law Review*, *32*(1), 145.

Ammous, S. (2016). *Blockchain technology: What is it good for?* http://dx.doi.org/10.2139/ssrn.2832751

Aponte-Novoa, F. A., Orozco, A. L. S., Villanueva-Polanco, R., & Wightman, P. (2021). The 51% Attack on Blockchains: A Mining Behavior Study. *IEEE Access*, *9*, 140549–40564. https://doi.org/10.1109/ACCESS.2021.3119291

Austin, T. H., & Di Troia, F. (2022). A Blockchain-Based Tamper-Resistant Logging Framework. In L. Bathen, G. Saldamli, X. Sun, T. H. Austin, & A. J. Nelson (Eds.), *Silicon Valley Cybersecurity Conference. SVCC 2022. Communications in Computer and Information Science* (vol. 1683, pp. 90–104). Springer, Cham. https://doi.org/10.1007/978-3-031-24049-2_6

Belotti, M., Božić, N., Pujolle, G., & Secci, S. (2019). A Vademecum on Blockchain Technologies: When, Which, and How. *IEEE Communications Surveys & Tutorials*, *21*(4), 3796–3838. https://doi.org/10.1109/comst.2019.2928178

Bertolini, A., Episcopo, F., & Cherciu, N.-A. (2021). *Liability of online platforms*. European Parliamentary Research Service (EPRS).

Cohen, J. E. (2017). Law for the platform economy. *UC Davis Law Review*, *51*, 133–204.

Finocchiaro, G. (2010). La memoria della rete e il diritto all'oblio. *Il Diritto Dell'informazione e Dell'informatica*, *3*, 391–404. (In Italian).

Golden, E. J., Najahi, J. J. V., & Jhanjhi, N. Z. (2020). *Blockchain Technology: Fundamentals, Applications, and Case Studies*. Taylor & Francis Ltd. https://doi.org/10.1201/9781003004998

Gramoli, V. (2022). *Blockchain Scalability and its Foundations in Distributed Systems*. Springer Cham. https://doi.org/10.1007/978-3-031-12578-2

Gupta, S., Gupta, A., Pandya, I. Y., Bhatt, A., & Mehta, K. (2023). End to end secure e-voting using blockchain & quantum key distribution. *Materials Today: Proceedings*, *80*, 3363–3370. https://doi.org/10.1016/j.matpr.2021.07.254

Kenney, M., & Zysman, J. (2016). The rise of the platform economy. *Issues in Science and Technology*, *32*(3), 61–69.

Kocharyan, H., Vardanyan, L., Hamuľák, O., & Kerikmäe, T. (2021). Critical views on the right to be forgotten after the entry into force of the GDPR: Is it able to effectively ensure our privacy? *International and Comparative Law Review*, *21*(2), 96–115. https://doi.org/10.2478/iclr-2021-0015

Lacity, M. C., & Treiblmaier, H. (Eds.) (2022). *Blockchains and the Token Economy: Theory and Practice (Technology, Work and Globalization)* (1st ed.). Palgrave Macmillan.

Mantelero, A. (2013). The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'. *Computer Law & Security Review*, *29*(3), 229–235.

Mccorry, P., Mehrnezhad, M., Toreini, E., Shahandashti, S. F., & Hao, F. (2021). On Secure E-Voting over Blockchain. *Digital Threats: Research and Practice*, *2*(4), 33. https://doi.org/10.1145/3461461

Michael, J., Cohn, A., & Butcher, J. R. (2018). Blockchain technology and regulatory investigations. *The Journal Litigation*, *1*, 35–44.

Nassar, M., Salah, K., & Svetinovic, D. (2019). Blockchain for explainable and trustworthy artificial intelligence. *WIREs Data Mining and Knowledge Discovery*, *10*(1), e1340. https://doi.org/10.1002/widm.1340

Peguera, M. (2019). The Right to Be Forgotten in the European Union. In G. Frosio (Ed.), *Oxford Handbook of Online Intermediary Liability*. Oxford University Press.

Pelosi, A., Felicioli, C., Canciani, A., & Severino, F. (2023). A Hybrid-DLT Based Trustworthy AI Framework. In *2023 IEEE International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)* (pp. 1–6). https://doi.org/10.1109/wetice57085.2023.10477792

Politou, E., Michota, A., Alepis, E., Pocs, M., & Patsakis, C. (2018). Backups and the right to be forgotten in the GDPR: An uneasy relationship. *Computer Law & Security Review*, *34*, 1247–1257. https://doi.org/10.1016/j.clsr.2018.08.006

Rajasekaran, A. S., Azees, M., & Al-Turjman, F. (2022). A comprehensive survey on blockchain technology. *Sustainable Energy Technologies and Assessments*, *52*, 102039. https://doi.org/10.1016/j.seta.2022.102039

Raymond Choo, K.-K., Dehghantanha, A., & Parizi, R. M. (Eds.) (2020). *Blockchain Cybersecurity, Trust and Privacy (Advances in Information Security* (1st ed.). Springer Cham. https://doi.org/10.1007/978-3-030-38181-3

Sarzana, F., & Nicotra, M. (2018). *Diritto della blockchain, intelligenza artificiale e IoT*. Ipsoa. (In Italian).

Smith, S. S. (2020). *Blockchain, Artificial Intelligence and Financial Services (Future of Business and Finance)*. Springer Cham.

Springer, A., Hollis, V., & Whittaker, S. (2017). Dice in the Black Box: User Experiences with an Inscrutable Algorithm. In *The AAAI 2017 Spring Symposium onDesigning the User Experience of Machine Learning Systems Technical Report SS-17-04* (pp. 427–430).

Stark, D., & Pais, I. (2020). Algorithmic management in the platform economy. *Sociologica*, *14*(3), 47–72. https://doi.org/10.6092/issn.1971-8853/12221

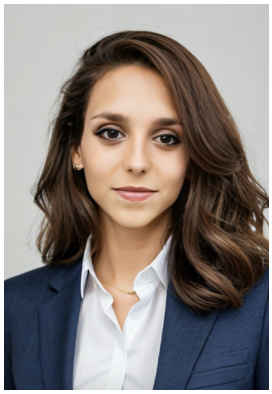
Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International*, *22*(4), 97–112. https://doi.org/10.9785/cri-2021-220402

Walch, A. (2016). The Path of the Blockchain Lexicon (and the Law). *Review of Banking and Financial Law*, *36*, 713–765.

Xue, C., Tian, W., & Zhao, X. (2020). The literature review of platform economy. *Scientific Programming*, *2020*(1), 8877128. https://doi.org/10.1155/2020/8877128

Authors information

Fabio Severino – CTO, Traent SRL
Address: Borgo Stretto 3, 56127, Pisa, Italy
E-mail: fabio.severino@traent.com
ORCID ID: https://orcid.org/0000-0002-9538-1218



Ludovica Sposini – PhD Candidate (Law), DIRPOLIS Institute (Institute of Law, Politics and Development), Sant'Anna School of Advanced Studies
Address: Via Domenico Vernagalli 22R, 56127 Pisa, Italy
E-mail: ludovica.sposini@santannapisa.it
ORCID ID: https://orcid.org/0000-0003-2188-8996
Google Scholar ID: https://scholar.google.com/citations?user=AVR7_bMAAAAJ

Authors' contributions

The authors have contributed equally into the concept and methodology elaboration, validation, formal analysis, research, selection of sources, text writing and editing, project guidance and management.

Conflict of interest

The authors declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Acknowledgements

The authors would like to thank Traent SRL for providing all the technical documentation concerning its technology for the purpose of this article. In addition, we would also like to thank the Jean Monnet Centre of Excellence on the Regulation of Robotics and AI (EURA) for the support.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – June 16, 2024
Date of approval – July 2, 2024
Date of acceptance – September 25, 2024
Date of online placement – September 30, 2024