



НАУЧНОЕ ПРИЛОЖЕНИЕ

Редакционная дата: 25 сентября 2026

Модель распределённых полномочий при отключении: пределы безопасного локального решения в услугах цифрового государства

Delegated Authority Under Network Partition:
An Exhaustive Toy-State Study and a Research
Protocol for Safe Offline Public Services

MERIDIAN FUTURES LAB | научное приложение M02 | рабочая статья 1.0 | редакционная дата: 25 сентября 2026 года

Фактический тип работы: критическая концептуальная статья с полностью выполненным ограниченным исчерпывающим исследованием пространства состояний (Conceptual Working Paper with an Executed Bounded Exhaustive State-Space Exploration). Она не представляется оригинальным операционным исследованием Саудовской Аравии, полным доказательством безопасности или рецензированной статьёй.

Граница доказательной базы: 25 сентября 2026 года. Предлагаемый срок программы: 2026–2035.

Русский реферат

В статье рассматривается вопрос, отличный от доступности услуги во время отключения: каков **предел локальных полномочий**, в котором цифровая система может действовать, не имея возможности мгновенно проверить общие реестры, и при этом сохранять инварианты прав и безопасность получателей? Мы различаем просмотр подписанной копии, предварительный приём заявления, реализацию редкого или уникального права и получение окончательного решения, подлежащего исполнению. Это различие сопоставляется с теорией согласованности как логической монотонности (Consistency as Logical Monotonicity; CALM), исследованиями устранения координации (Coordination Avoidance), пределами сходимости распределённых копий данных в бесконфликтных реплицируемых типах данных (Conflict-Free Replicated Data Types; CRDT) и задачами проектирования автономных платежей в проекте Polaris (Project Polaris).

Используются три группы свидетельств: отключение электроэнергии на Пиренейском полуострове 28 апреля 2025 года и зафиксированные Банком Испании (Banco de España) и Европейским центральным банком (European Central Bank; ECB) перебои платёжных каналов, преимущества наличных и пределы их распределения; сохранение части функций Британской библиотеки (British Library) при недоступности других после атаки в октябре 2023 года; опубликованные нормы Саудовской Аравии об управлении непрерывностью бизнеса в банковском секторе и цифровом правительстве. Ни одна из этих групп не позволяет оценить вероятность отказа услуги Саудовской Аравии или её реальные локальные полномочия, но они помогают сформулировать проверяемые вопросы.

Мы выполнили полный вычислительный перебор состояний **ограниченной синтетической модели**: два разобшённых узла, три общие единицы права, пять возможных уровней локального спроса в каждом узле — от нуля до четырёх — и пять политик принятия решений. Это **25 состояний спроса и 125 оценок политик**. При политике слепого локального подтверждения общий предел был нарушен в **13 из 25 состояний**. Разделение полномочий на две единицы и одну сохранило предел во всех состояниях при допущении добросовестного локального исполнения, но, если сложить различия по всем состояниям, привело к потере **десяти совокупных единиц безопасного исполнения** по сравнению с базовым вариантом при постоянной связи. Это **исчерпывающий подсчёт заданных абстрактных состояний**, а не статистическая вероятность и не вывод о реальном учреждении. Отдельный пример показывает, что одной действительной криптографической подписи недостаточно, чтобы не допустить использования копии одного жетона в двух местах без координации или соответствующих аппаратных гарантий.

Статья предлагает операционный профиль полномочий каждой услуги при отключении (Offline Authority Profile; OAP) и протокол санкционированного испытания, в котором сопоставляются сохранность прав, фактическое исполнение, накопившиеся

запросы, социальная справедливость и стоимость проверки. Её вклад — в упорядочении вопросов, условий и испытаний, а также в выявлении ситуаций, где остановка или временное обещание честнее и безопаснее необратимого завершения.

Ключевые слова: ограниченные локальные полномочия (Bounded Local Authority); разделение сети (Network Partition); прикладные инварианты (Application Invariants); устранение координации (Coordination Avoidance); распределение резерва (Escrow Allocation); двойное расходование (Double Spending); действительность подписи (Signature Validity); последующее согласование (Reconciliation).

English abstract

The research question is **which public-service decisions can be safely authorized locally during a network partition**, rather than simply which interfaces remain operational. A distinction is made among viewing signed and time-bounded information, receiving provisional intent, consuming preallocated scarce authorization, and making final decisions that require shared, fresh knowledge. The synthesis draws on CALM, invariant-confluent coordination avoidance, conflict-free replication, and the Bank for International Settlements' Project Polaris research on offline payment design. Documented case evidence covers the April 2025 Iberian blackout and payment disruption, the British Library's post-2023 partial-service restoration, and Saudi rules on institutional business continuity.

An **executed, fully synthetic, bounded exhaustive analysis** explores 25 demand states at two disconnected sites under five decision policies. The global scarce authorization budget equals three invented units. Blindly letting each site independently commit against the old global balance violates the shared quota in 13 of 25 cases. Honest, disjoint escrow allocation preserves the quota in all enumerated cases but yields 10 fewer safely finalized units in aggregate than an always-connected benchmark. These are **counts of constructed abstract states, not estimated risks, probabilities, Saudi results, or guarantees against adversarial compromise**. A separate replay counterexample illustrates why a valid issuer signature alone does not ensure unique offline redemption. We propose an Offline Authority Profile and an authorized measurement protocol with explicit outcomes, safety invariants, revocation constraints, appeal handling, and distributional assessment.

Keywords: offline public services; delegated authority; safety invariants; network partition; application semantics; bounded escrow; digital identity; payment resilience; Saudi Arabia.

1. Единица анализа: действие, изменяющее право

Многие обсуждения непрерывности бизнеса (Business Continuity) сводятся к инфраструктурной лексике: второй сервер, резервная зона, запасной канал связи, ограниченный режим. Это важные средства, но они не дают прямого ответа на вопрос о **правомерности последствий действия**, если необходимые для него общие сведения недоступны. Устройство может принимать заявления локально, но приём заявления не

равнозначен окончательному распоряжению юридическим или финансовым правом. Поэтому мы выбираем другую единицу анализа: **санкционированное действие, изменяющее состояние (Authorized State-Changing Action)**, либо чтение, которое состояние не изменяет и должно сообщать, насколько свежи подтверждающие его данные.

Основной вопрос: **при каких правовых, информационных, криптографических и операционных условиях подразделение, узел, устройство или представитель услуги может завершить определённое действие во время отключения от общей власти неизвестной длительности, не превысив переданных ему полномочий и не создав неисправимого противоречия?**

Мы выделяем пять дополнительных вопросов:

1. Какие решения остаются правильными после поступления новых сведений, а какие зависят от знания об отсутствии права или ограничения в удалённом месте?
2. Чем действительность криптографической подписи отличается от права использовать ресурс или мандат только один раз?
3. Как разделить редкое право между независимыми узлами, не допустив нарушения инвариантов общего реестра? Какова цена неиспользованных долей?
4. Когда предварительная регистрация намерения приносит общественную пользу и при этом не превращает квитанцию в ложное обещание окончательного исполнения?
5. Как испытывать локальные возможности с учётом права, регулирующего услугу, реальной доступности для людей и неравномерного распределения устройств, электричества и времени?

Цель статьи — концептуальная и проектная, с завершённым иллюстративным вычислительным компонентом. В этой версии мы не проверяем причинно-следственные связи на уровне страны, не выводим частоты отказов или воздействий и не подтверждаем безопасность реальной платёжной системы. Функциональная оценка отделяется от правовой, технической и социальной. Способность автомата состояний сохранить численный предел не даёт ему права на институциональное применение.

Гипотезы и опровергающие показатели

H1 — условное предварительное делегирование: инварианты некоторых действий можно сохранять локально посредством ограниченного, обособленного мандата уполномоченной инстанции при наличии свидетельств, подписи, аудита и ясного сообщения пользователю о состоянии его запроса.

H2 — пределы незнания во время отключения: другие действия требуют свежего знания реестра или исключительности ресурса. Если каждый узел получает право пользоваться одной и той же устаревшей копией, могут возникнуть лишние или противоречащие друг другу права.

H3 — цена пределов: предварительное распределение может гарантировать исключительность и уменьшить вред, но оно замораживает доли в узлах, где во время кризиса они не нужны, и лишает другие узлы допустимых действий, которые были бы возможны при координации.

H4 — польза временного обещания: документированный предварительный приём может сохранить момент подачи запроса и право заявителя на рассмотрение, но он не заменяет окончательного исполнения и подходит не для всякого права.

H5 — возможное возражение: для большинства чувствительных функций наилучшим решением может оказаться безопасная остановка, ограниченный защищённый канал связи или усиленный переход к очному обслуживанию вместо сложного локального делегирования. Эти варианты должны оставаться частью сравнения.

Тезис о практической пользе будет опровергнут, если санкционированные испытания покажут, что с учётом атак, исправления прав и расходов конкретный локальный мандат не увеличивает число корректно завершённых действий по сравнению с временной остановкой либо создаёт недопустимую для государственной политики несправедливость доступа.

2. Основания знания: от связи к смыслу действия

2.1 Почему репликации данных недостаточно?

Исследования распределённых систем (Distributed Systems) описывают среду, где работают независимые устройства, а сообщения между ними могут задерживаться или не доходить. В такой среде слово «правильно» имеет несколько значений. Оно может означать, что после последующего соединения копии показывают одно значение. А может означать, что каждое решение пользователя или учреждения во время разрыва соответствовало правилу, которое нельзя нарушать ни в один момент. Первая цель может быть достигнута уже после нарушения второй.

Марк Шапиро (Marc Shapiro) и его соавторы в работах о бесконфликтных реплицируемых типах данных (Conflict-Free Replicated Data Types; CRDT) показали, что при определённых условиях можно проектировать распределённые типы данных, копии которых сходятся после обновлений. Но это инструменты, гарантирующие конкретные свойства слияния. Самих по себе их недостаточно, чтобы сформулировать закон редкого права или обязанность не выдавать его дважды. [S10](#)

2.2 Что можно делать без координации?

Теория согласованности как логической монотонности (Consistency as Logical Monotonicity; CALM) связывает некоторые логические формы операций с возможностью исполнять их без постоянной координации, сохраняя согласованный смысл. Джозеф

Хеллерстайн (Joseph M. Hellerstein) и Питер Альваро (Peter Alvaro) излагают это различие и рассматривают его значение для проектирования распределённых программ. [S08](#)

Монотонность здесь — техническое понятие. При подходящей логической формулировке добавление новых входных данных к уже имеющемуся набору не должно заставлять программу отзываться ранее доказанные результаты так, что нарушается её условие. Поэтому зарегистрировать независимое событие или добавить соответствующий требованиям документ проще, чем принять решение, которое зависит от отсутствия какого-то события во всей остальной системе. Но не всякое «добавление» безопасно: удаление последствия, отзыв разрешения и выравнивание ресурсов могут изменить вывод.

Питер Бейлис (Peter Bailis) и его соавторы в работе об устранении координации (Coordination Avoidance in Database Systems) предложили критерий, связанный с прикладными инвариантами, — **инвариантную сходимость (Invariant Confluence; I-Confluence)**. Для наших целей важно не довольствоваться сходимостью копий, а установить, может ли слияние двух локально корректных состояний нарушить глобальное условие корректности. Работа прямо различает доступность и сходимость, с одной стороны, и гарантии сохранности прикладных инвариантов — с другой. [S09](#)

В услугах цифрового государства инвариант может требовать не пользоваться разрешением после отзыва, не выдавать одну долю пособия дважды или не закреплять уникальную запись более чем за одной стороной. До того как стать программным условием, эти инварианты должны получить юридическое определение. Исследователь не вправе придумать правило выдачи и считать, что оно обязательно для всех учреждений.

2.3 Автономные платежи — не готовый рабочий режим

В 2023 году Банк международных расчётов (Bank for International Settlements; BIS) выпустил в рамках проекта Polaris (Project Polaris) руководство по автономным платежам цифровыми валютами центральных банков. В нём конфиденциальность, доступность, безопасность устройств, пределы хранения и расходования, операционные правила и риск повторного использования рассматриваются как проектные решения, для которых нет одного универсального варианта. В последующем документе от октября 2023 года отмечалось, что многие решения тогда оставались на стадии эксперимента или разработки, а готовых к широкому практическому внедрению было немного. [S06S07](#)

Европейский центральный банк (European Central Bank; ECB) в августе 2026 года объявил консультации о стандартах защищённых элементов и встроенных SIM-карт в рамках планирования автономных платежей цифровым евро. На текущей границе

доказательной базы сам цифровой евро **не является общедоступной валютой**; возможный выпуск в последующие годы зависит от законодательства, решений и испытаний. [S16S17](#)

Эти источники делают тезис уже и точнее. Полномочия, переданные устройству, требуют реального управления редкостью, защиты от копирования и проверки личности уполномоченного. При этом после изменения в недоступном центре остаются свойства, которые невозможно проверить локально, в том числе некоторые случаи отзыва и одновременной передачи через независимые устройства.

3. Свидетельства реального мира: три разные единицы наблюдения

3.1 Испания и Португалия 28 апреля 2025 года

В обзоре от 27 апреля 2026 года Банк Испании (Banco de España) зафиксировал, что крупное отключение электроэнергии началось около 12:33 28 апреля 2025 года и нарушило электронные платежи и работу банкоматов, тогда как наличные, уже находившиеся у людей, оставались средством прямого обмена, не требовавшим электричества или связи в реальном времени. В обзоре также сказано, что часть банкоматов не работала, хотя в них были деньги, а 29 и 30 апреля банк совместно с перевозчиками наличности пополнял банкоматы. [S01](#)

Европейский центральный банк (European Central Bank; ECB) в исследовании 2025 года сообщает, что по указанным сопоставлениям платежи по картам в физических точках пострадавших районов сократились примерно на 41–42%, а онлайн-покупки — примерно на 54%. Данные CaixaBank Research, основанные на выборке операций и сравнительных исследованиях, оценили снижение отражаемых их показателями потребительских расходов в день отключения примерно в 34%; часть разрыва была компенсирована в последующие дни. Эти проценты не представляют собой рандомизированный эксперимент или меру всей экономической активности: различия между регионами, отложенные покупки и охват данных учреждения влияют на их трактовку. [S02S04](#)

20 марта 2026 года Европейская сеть операторов систем передачи электроэнергии (European Network of Transmission System Operators for Electricity; ENTSO-E) опубликовала итоги расследования отключения на Пиренейском полуострове, сосредоточенные на нескольких взаимодействующих факторах энергосистемы. Мы не истолковываем причины отключения через нашу теорию цифровых полномочий. Событие используется как **документированное внешнее отключение**, которое проявило платежи, зависевшие от разрешения недоступной сети. [S03](#)

3.2 Британская библиотека в 2023–2025 годах

После кибератаки на Британскую библиотеку (British Library) в октябре 2023 года её здания и читальные помещения оставались доступными, а возможности поиска, каталогизации и электронные услуги были нарушены. В марте 2024 года учреждение выпустило собственный обзор, а в 2025 году — сообщения о постепенном восстановлении услуг. Доступные материалы не подтверждают, что использовалась какая-либо особая модель «локальных полномочий». Они показывают только, **что продолжение одной части миссии учреждения может сосуществовать с крупной, открыто признанной утратой другой.** [S14S15](#)

3.3 Саудовская Аравия как место постановки вопроса, а не предполагаемый случай отказа

На нормативном сайте Центрального банка Саудовской Аравии (Saudi Central Bank; SAMA) размещены рамочная модель управления непрерывностью бизнеса, опубликованная в 2017 году, и инструкции 2021 года о резервном электроснабжении банков, проверке генераторов, их мощности и обслуживания. Управление цифрового правительства (Digital Government Authority; DGA) также публикует регулирующие материалы и справочные руководства об управлении рисками и непрерывностью цифрового правительства, в том числе контрольные требования версии 2.0 и последующее руководство. [S11 \(связанное руководство 2025 года\)](#)[S12S13](#)

Эта программа не имеет доступа к журналам отказов или внутренним полномочиям. Мы не делаем выводов о том, что чувствительное приложение Саудовской Аравии лишено локального мандата или использует одну из описанных нами форм. Наличие норм непрерывности указывает на внимание институтов к теме, но не доказывает, какие действия можно законно и операционно завершать без связи и к каким результатам привели учения.

Таблица пределов вывода

Группа	Что подтверждает источник	Роль в исследовании	Какого утверждения источник не допускает
Пиренейский полуостров, 2025	Масштабное отключение электричества и сбои некоторых платёжных каналов; пригодность имевшихся у держателя наличных для обмена	Показывает независимость некоторых видов расчёта от сетей разрешения в реальном времени	Что наличных хватает всем пользователям или все цифровые платежи пострадали одинаково
Британская библиотека, 2023–2025	Читальные пространства продолжали работать, а поиск и каталогизация были нарушены на долгий срок	Показывает неодинаковые уровни полномочий и операций, которые можно сохранить	Что частичная работа устранила последствия атаки или применялся документ локального делегирования
Нормы Саудовской Аравии	Официальная основа управления, испытаний и резервирования в указанных секторах	Определяет институциональную основу для предложения исследовательского сотрудничества	Что автономные исполнительные модули проходили опубликованные испытания или доказали успех

4. Концептуальная модель: решение как информация, полномочие и свидетельство

Обозначим действие услуги через a , желающую завершить его сторону через i , а момент времени через t . Локальное решение требует проверки по меньшей мере четырёх элементов:

- 1. Правомерность действия (Authorization):** полномочия учреждения, устройства или сотрудника совершить определённое действие в признанной сфере компетенции.
- 2. Целостность свидетельства (Evidence Integrity):** источник и подпись, неизменность копии или заявления, действительность проверочных ключей в соответствующей политике.
- 3. Свежесть условия (Freshness):** время выпуска данных, риск их изменения или отзыва во время отключения и допустимая продолжительность такого незнания.
- 4. Сохранность инварианта (Invariant Safety):** действие не должно создавать двойное право, долг или запрещённое изменение после объединения с результатами других узлов.

В предлагаемой проектной схеме разрешение локального действия можно представить логическим условием:

$$\text{ALLOW}(a, i, t) = A(a, i, t) \wedge E(a, i, t) \wedge F(a, t) \wedge I(a, i, t).$$

Если одно из условий равно нулю, **завершение** по этому правилу должно остановиться; предварительный приём, объяснение или передача запроса по другому пути при этом могут оставаться возможными. Это концептуальная формула, а не готовая машина юридических решений. Каждую функцию необходимо определить и в необходимой мере связать с нормативными источниками, испытаниями и опубликованными данными.

Мы не приравниваем подпись к правильности всех элементов свидетельства. При корректной криптографической модели подпись может доказать, что сообщение не изменили и оно выпущено определённым ключом. Но сама по себе она не доказывает, что предъявитель всё ещё обладает правом, ключ не был отозван во время отсутствия связи или сообщение не использовали в другом месте. Такая уязвимость не обязана присутствовать во всякой архитектуре: её можно уменьшить короткоживущими мандатами, распределёнными долями, защищённым оборудованием, пределами стоимости и использования, аудиторским журналом. Но всякая мера добавляет новые расходы и условия доверия.

4.1 Необходимое различие между правильностью решения и продолжением взаимодействия

Мы различаем четыре вида результата:

- **Completed Valid:** корректное окончательное действие в пределах объявленного и проверяемого мандата.
- **Accepted Provisional:** заявление принято с квитанцией, где указано, что оно ожидает проверки или согласования.
- **Deferred or Escalated:** заявление приостановлено с указанием причины, ясного состояния, срока проверки или канала помощи.
- **Rejected or Unsafe:** обоснованный отказ из-за отсутствия полномочий или свидетельства либо неудавшаяся попытка, разрешение которой нарушило бы условие.

Нельзя складывать все четыре вида в число «завершённых операций». Справедливость также требует не считать предварительный приём безусловной неудачей: если политика придаёт квитанции реальное, пусть и не окончательное значение, она может сохранить место правообладателя в очереди и момент подачи. Но оценка зависит от правового контекста и характера вреда от отсрочки.

5. Сохранение редкого права: от невозможной координации к условному разделению

Начнём с намеренно простой модели, которую легко проверить. Имеется ограниченный общий объём в некоторого права. До отключения уполномоченная центральная инстанция выдаёт независимым узлам непересекающиеся доли q_i .

Каждый узел может завершать использования c_i только в пределах своей доли. Если выполняются условия:

$$q_i \geq 0, \quad c_i \leq q_i, \quad \sum_i q_i \leq B,$$

то:

$$\sum_i c_i \leq \sum_i q_i \leq B.$$

Это корректное рассуждение **внутри модели**, при условии, что доли нельзя подделать или повторить, локальное состояние хранится добросовестно, а все участники следуют одному правилу использования. Это не доказательство безопасности реальной системы: модель не рассматривает потерю устройств, клонирование оборудования, совместное использование ключей, атаки повторного воспроизведения, отзыв ранее выданного мандата и решения людей, выходящие за рамки политики. Эти условия не мелкая оговорка: нарушение любого из них способно разрушить сам предел.

Механизм похож на предварительное резервирование или распределение резерва (Escrow Allocation): отпадает необходимость спрашивать разрешение на каждое движение, потому что часть права на движение получила известные пределы и исключительно закреплена за одним местом. Но у этого преимущества есть цена: **доли распределяются до того, как станет известен фактический спрос во время отключения**. Узел «А» не может по собственному желанию передать себе неиспользованное право из «Б», иначе потребуются связь или новый протокол, гарантирующий, что передача не повторилась.

5.1 Почему устаревшего остатка в двух узлах недостаточно?

Если перед отключением оба узла сохранили общую копию со словами «осталось три единицы», а затем каждый разрешил себе потратить по три, итог составит шесть. Обе стороны добросовестно действуют по своей локальной копии, но нарушают общий предел. Это **типовой контрпример (Counterexample)**, возникающий из-за отсутствия координации при хранении неделимой копии редкого ресурса. Его следует отличать от реальных денег: финансовая система может иметь другие правила, расчёты, оборудование и гарантии, которых наша модель не воспроизводит.

5.2 Почему действительность подписи не означает уникальность погашения?

Мы реализовали отдельный пример с одним копируемым цифровым жетоном t_1 , имеющим действительную подпись эмитента и известным двум разобщённым точкам. Если каждая точка не видит журнал использования другой, а жетон не привязан к неклонируемому оборудованию или исключительному месту использования, каждая

может принять его один раз. Подпись при этом действительна в обоих случаях, но условие **единственного глобального использования** нарушено. Это состояние явно записано в `data/duplicate_token_counterexample.json`.

Это не означает, что всякая подпись или защищённый цифровой кошелёк подвержены одной и той же атаке. Пример показывает, почему утверждение «подпись предотвращает двойное расходование без связи» должно указывать архитектуру оборудования, привязку остатка или долей и ограничения копирования. Документы проекта Polaris (Project Polaris) различают решения и риски в зависимости от архитектуры и отводят центральное место защищённым элементам и операционным пределам. [S06S07](#)

6. Выполненный вычислительный эксперимент: 25 состояний × пять политик

6.1 Полнота перебора и пределы утверждений

Программа полностью перебрала **заранее заданное множество состояний**. Это не эксперимент Монте-Карло (Monte Carlo Simulation) и не выборка учреждений. В каждом состоянии независимое число запросов в узлах «А» и «Б» принадлежит множеству $\{0, 1, 2, 3, 4\}$, поэтому число пар равно $5 \times 5 = 25$. Общий объём права $v=3$ синтетические единицы. Каждая пара оценивается при пяти политиках. Для пар не заданы вероятности возникновения, веса населения, длительность отключения или рабочие криптографические операции; модель не содержит человеческого поведения.

6.2 Пять политик

P0 — Central Stop: все окончательные подтверждения ждут связи с центром; в период изоляции ничего не исполняется. Другое учреждение может продолжать предоставлять сведения или помощь, но это находится за пределами численного расчёта.

P1 — Provisional Intake: система регистрирует все намерения как предварительно принятые; они не считаются окончательно исполненными и ожидают проверки после восстановления связи.

P2 — Escrow (1,2): одна единица зарезервирована для «А», две — для «Б». У каждого узла есть предел, который нельзя превысить без связи; лишние запросы остаются в очереди на проверку.

P3 — Escrow (2,1): точная противоположность, позволяющая проверить последствия решения выдать одному региону вдвое большую долю до того, как известно распределение спроса.

P4 — Blind Local Commit: каждый узел исполняет до трёх единиц, словно только он расходует весь общий ресурс. Политика служит для выявления нарушающего поведения и не предлагается как приемлемый профессиональный вариант.

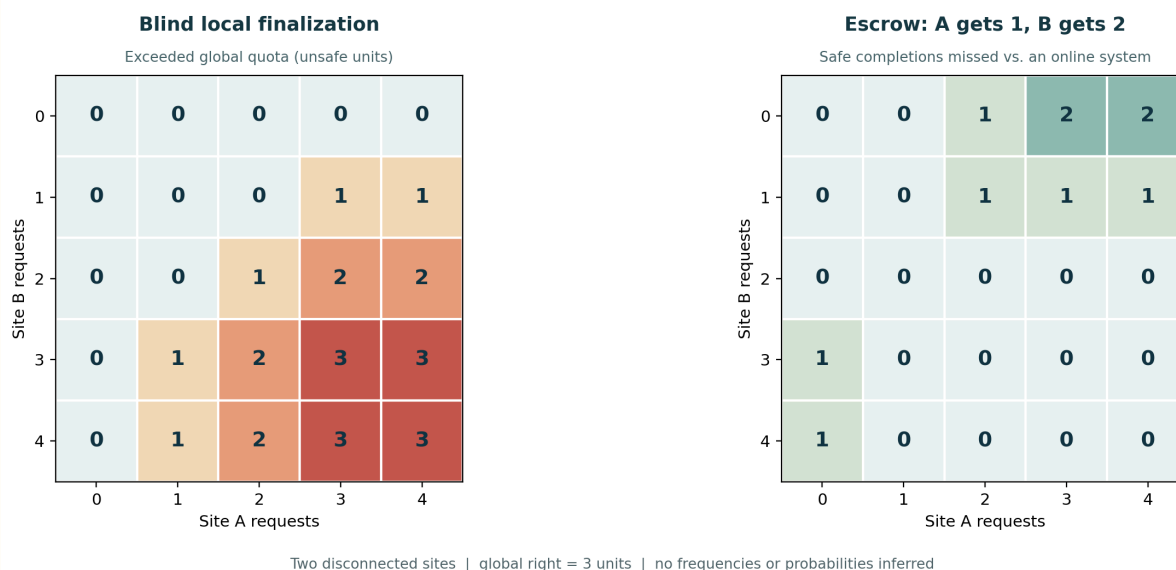
Связанный базовый вариант после получения обоих значений спроса способен исполнить в каждом состоянии $\min(3, d_A + d_B)$ единиц. Модель не учитывает время ожидания, операционные расходы и длительность проверки, поэтому не пригодна для финансового сравнения и описания реальной продолжительности отключения.

6.3 Воспроизводимые результаты

Политика	Испытанные состояния	Состояния с превышением предела	Наибольшее превышение в единицах модели	Всего исполнений по 25 состояниям	Всего предварительных намерений	Дефицит безопасного исполнения относительно связанного варианта
Центральная остановка P0	25	0	0	0	0	65
Предварительный приём P1	25	0	0	0	100	65
Резерв (1,2) P2	25	0	0	55	45	10
Резерв (2,1) P3	25	0	0	55	45	10
Слепое подтверждение P4	25	13	3	90	0	0*

*В строке P4 ноль в столбце дефицита не означает безопасную работу: политика превышает общий объём права в 13 состояниях, и часть её подтверждений недействительна. Все суммы складывают показатели по **взаимоисключающим альтернативным состояниям**, а не операции или людей, существовавших одновременно. Значение 13/25 нельзя трактовать как вероятность отказа в 52%.*

Twenty-five EXHAUSTIVE, SYNTHETIC request states



Две карты нарушений предела и упущенных возможностей при разделённом мандате

Рисунок 2. Состояние на каждой оси задаёт число запросов одного узла; всего на карте 25 ячеек. Первая карта показывает величину превышения права, вторая — число упущенных безопасных исполнений при фиксированном разделении 1+2 относительно полного знания связанной системы. Значения получены непосредственно программой и не содержат данных Саудовской Аравии.

6.4 Контрпример и преимущество, о котором нельзя забывать

Если узел «А» запрашивает три единицы, а «Б» — ни одной, резерв (1,2) исполняет одну единицу. Тем самым «А» лишается двух возможностей безопасного исполнения, которые центр реализовал бы, не превышая предела. Это **цена планирования до появления спроса**. Её можно уменьшить, перераспределяя доли при наличии связи до кризиса, делая разделение более дробным или создавая ограниченный канал передачи мандата при наличии правовых и технических гарантий. Нельзя утверждать, что проблема редкости решена простым копированием остатка.

В обратном примере, когда каждый узел запрашивает две единицы, слепая политика разрешает исполнить четыре, хотя общий объём права равен трём. Разделённый резерв сохраняет предел, но может отказать одному из запросов или заставить его ждать. Правильный выбор зависит от цены несправедливости и задержки, объявленных правил приоритета и природы права, а не просто от максимизации столбца «исполнено» в панели показателей.

6.5 Что действительно проверено, а что не происходило

Код был запущен и создал `model_check_states.csv` со 125 строками, `model_check_summary.csv` для пяти политик, файл допущений, журнал нарушения с копируемым жетоном и два оригинальных рисунка. Программа проверяет вычислительные утверждения: ни одна схема добросовестного резервирования не превышает предел в заданных состояниях; число строк равно 125; слепая политика действительно создаёт нарушения. **Это испытание небольшой программной модели.** Оно не испытывает устройства, платёжные протоколы или хранение ключей и не создаёт комплексной институциональной гарантии.

Мы не проверяли чувствительность, добавляя группы населения или выбирая вымышленное вероятностное распределение. Прикладное исследование потребует повторного запуска на санкционированных реальных долях спроса, с учётом стоимости различных приоритетов, ограничений хранения и батареи, потери связи, отзыва ключей, украденных кошельков и целостности аудита.

7. Передать полномочие — не то же самое, что оснастить устройство

7.1 Отзыв и временной предел

Подписанный документ мог быть действительным в момент выдачи, а указанное в нём право — отозвано во время отключения. Рассмотрим две возможные истории системы: в n_0 отзыва не было; в n_1 отзыв произошёл в центре, которого локальное устройство не слышит. Если все видимые устройству входные данные в этих историях одинаковы, один лишь локальный алгоритм не определит, какая история истинна. Нужна объявленная политика, задающая допустимый возраст свидетельства; либо действие, которое остаётся правильным при изменении состояния; либо канал связи или полномочие с более коротким сроком; либо остановка окончательного исполнения.

Машинное обучение не преодолеет это незнание простым прогнозом вероятности отзыва: несанкционированное решение от прогноза не становится санкционированным. Модель искусственного интеллекта (Artificial Intelligence; AI) может помочь расставить дела по приоритету проверки или обнаружить противоречия после восстановления связи, но не создаёт источник законной власти и не доказывает невидимую ей информацию.

7.2 Право, которым держатель не может воспользоваться во время кризиса

Пользователь может иметь цифровой документ, доступный без связи, но ему всё равно нужен тот, кто примет документ в соответствии с законом и практикой учреждения. Платёжная карта может локально проверить некоторые сведения, а терминал продавца

— не работать без электричества. Поэтому испытывать нужно всю систему: источник, устройство, сотрудника, свидетельство получателя, канал жалобы, местное электроснабжение и дальнейшую судьбу квитанции.

7.3 Конфиденциальность и дискриминация

Автономный режим может помочь пользователям там, где связь хуже, но исключить тех, у кого нет современного устройства, действительного документа или заранее внесённого остатка. Упор на синхронизируемые аудиторские журналы может привести к передаче лишних персональных данных, которые не требуется собирать. Нужны минимизация данных, параллельные человеческие пути и измерение различий между подходящими регионами и группами при соблюдении защиты конфиденциальности и санкционированного участия. Общий средний показатель скорости не должен скрывать пользователя, которому не оставили доступного пути.

7.4 Не все последствия можно исправить

Можно исправить порядок очереди или объединить две заметки в журнале. Но последствия передачи уникального предмета неуполномоченному человеку, небезопасного медицинского решения или юридического распоряжения, на которое у исполнителя не было окончательных полномочий, могут оказаться неисправимыми. Критерий «можно синхронизировать позднее» описывает информационную возможность, а не всегда способность вернуть социальные и правовые отношения в прежнее состояние.

8. Проект санкционированного полевого исследования в Саудовской Аравии

8.1 Выборка и единица регистрации

Мы предлагаем добровольное санкционированное партнёрство с учреждениями, в чьих услугах можно проводить изолированные учения или использовать отдельные испытательные среды, не нарушая работу реальной публичной услуги. Единицей наблюдения должна стать **категория действия в санкционированном окне испытаний**, а не имя сервера или адрес чувствительного объекта. Действия классифицируются по юридическим последствиям: чтение, приём, резервирование ресурса, обратимое завершение и высокоэффективное завершение, которое возможно только в центре.

8.2 Переменные, которые следует собирать

Переменная	Необходимое операционное определение	Возможный санкционированный источник	Ограничение защиты или толкования
Вид действия	Запрос сведений, приём, выдача, расходование или отзыв?	Политика и спецификация услуги	Исследователь не меняет реальные категории полномочий
Локальный мандат	Вид разрешающего документа, его временной, предметный и количественный предел	Обезличенные утверждённые документы учреждения	Секреты ключей и места их хранения не публикуются
Свежесть свидетельства	Время последней проверки данных и полномочий	Агрегированные локальные журналы испытаний	Траектории записей отдельных людей не публикуются
Корректное завершение	Окончательное решение, соответствующее выбранной до эксперимента политике	Правовая и операционная проверка результатов	Не приравнивается к предварительному приёму
Предварительная квитанция	Сохранённый запрос с подтверждением времени, защитой от подмены и контекстом дальнейшего рассмотрения	Экспериментальные или синтетические журналы	Право не объявляется принятым до согласования
Противоречие	Расхождение между локальными решениями или с более поздним реестром	Синтетические события в защищённой среде	Классификация реального вреда требует одобрения специалиста
Проверка и возмещение	Срок разрешения спора и способ уведомления получателя	Испытания процедур учреждения	Недопустимо предполагать, что всякая ошибка устраняется автоматически
Справедливость	Различия в возможности подать или завершить запрос между уместными группами	Агрегированные показатели с защитой приватности	Чувствительные признаки не выводятся без необходимости и основания
Операционные расходы	Обучение, оборудование, проверка, задержка и помощь людям	Агрегированные внутренние финансовые данные	Сравниваются только однородные расходы

8.3 Схема сравнения

Для каждой однородной категории в испытательной среде сравниваются заранее определённые политики: остановка окончательного исполнения, предварительный приём, доли локального мандата, если это законно и возможно, и, вероятно, резервный канал связи. После одобрения синтетические сценарии внутри испытания можно

распределять случайно, сохраняя одинаковые виды запросов, доли и предполагаемую длительность обрыва. Мы не рекомендуем намеренно подвергать реальных пользователей или действующие юридические права превышению предела ради эксперимента.

Основные результаты: число корректных действий, завершённых в законных пределах; число обнаруженных и предотвращённых попыток нарушить инвариант; время урегулирования ожидающих квитанций; число случаев, которые нельзя согласовать без участия человека; агрегированные различия доступа; полная стоимость. Допустимые пределы следует задать **до** просмотра результатов сравнения, а всякое отклонение от плана анализа — зарегистрировать.

Допустимый конкурирующий результат: исследование может показать, что ограниченный резервный канал, усиление человеческих каналов общения или остановка определённых действий полезнее и безопаснее распределённого мандата. Тогда рекомендации должны следовать доказательствам; исследование не обязано доказывать пользу модели, желательной её автору.

8.4 Испытание против нарушителя и проверка безопасности

В санкционированной защитной среде следует проверить такие состояния: просроченное свидетельство; документ, отозванный во время отключения; повторно предъявленный жетон; потерянное устройство; ненадёжные часы; разный порядок поступления обновлений; предварительно принятая квитанция, которую затем невозможно исполнить; частичное восстановление связи, не охватывающее все реестры; повторный обрыв во время согласования. Общедоступный исследовательский отчёт не требует публиковать сведения о ключах, критической топологии или процедурах, позволяющих выбрать целью конкретный объект или услугу.

9. Профиль полномочий при отключении (ОАР): проектное предложение

Мы предлагаем создать структурированный институциональный реестр для каждого чувствительного действия, а не просто приложение к плану аварийной работы. Он отвечает на семь связанных вопросов: **право, носитель полномочий, свидетельство, его временной охват, пределы использования, правила остановки, порядок согласования и обжалования**. Схематически его можно представить так:

Предлагаемое поле	Минимальное содержание	Признак отказа, требующий внимания
authority_source	Основание мандата и норма, разрешающая действие	Полномочие не определено или субъект вышел за свою компетенцию
action_class	Запрос, приём, резервирование, завершение, передача на рассмотрение	Окончательное действие названо «временным запросом» или наоборот
evidence_policy	Источник, подпись, действительность данных и время обновления	Проверена просроченная подпись или отозванное свидетельство
scarcity_guard	Исключительный предел, предотвращающий превышение невозпроизводимого ресурса или права	Клонируемые жетоны или доли
stop_rule	Условия недостатка свидетельств, противоречия или невозможности обеспечить справедливость	Завершение продолжается несмотря на нарушение обязательного инварианта
reconnect_policy	Журнал событий, согласование, аудит, уведомление и обжалование	Тихое слияние скрывает вред и затронутого пользователя
inclusion_path	Помощь человека или материальный путь и справедливый срок для отложенных прав	Продолжение услуги доступно только определённому классу устройств или пользователей

Эта карточка — **предварительное предложение для исследования и проверки**, а не государственный стандарт и не итог семинара с реальными учреждениями. Её следует разрабатывать вместе со специалистами по праву, идентификации и безопасности, используя существующие стандарты и нормы Саудовской Аравии, но не заявляя о принадлежности или одобрении какой-либо организации.

10. Экономические и стратегические последствия до 2035 года

Мы не сводим экономический эффект к «числу часов доступности услуги». Учреждение может выполнить без связи пятьдесят действий, а затем дорого заплатить за согласование пяти необратимых ошибок. Оно может отложить лишь несколько действий, но настолько важных, что общественная цена ожидания многократно возрастёт. Поэтому статья предлагает **границу многокритериального выбора (Multi-Objective Decision Frontier)**, включающую корректное исполнение, исключительность, срок отсрочки, возможный вред, стоимость и различия доступа. До согласования весов и правомерности сравнения мы не строим единый составной показатель страны.

В перспективе для Саудовской Аравии есть четыре условных направления исследований и политики:

- 1. Полная централизация окончательных действий с каналами предварительного приёма.** Она может быть лучшим выбором, если невозможно гарантировать исключительность или закон не допускает делегирования. Потребуются ясные стандарты квитанций, сохранение запроса и времени подачи, механизмы обжалования.
- 2. Предварительно разделённые доли полномочий для узко определённых действий.** Они могут быть полезны при управляемых пределах и убедительных аудиторских испытаниях, но оплачиваются неподвижностью доли во время обрыва связи.
- 3. Делегирование на основании краткосрочных подписанных свидетельств.** Оно может подходить для показа сведений или действий с ограниченными последствиями, но сталкивается с риском недавнего отзыва и небезопасного хранения ключей. Математическая проверяемость подписи сама по себе не делает архитектуру правомерной.
- 4. Разработка национальных продуктов для управления профилем полномочий и согласованием.** Возможная сфера для программ испытания и моделирования действий и прав. Однако рынок подтверждается продажами продукта, повторными проверками его безопасности и работы у клиентов, а не картой страны со стрелками.

Это не прогнозы с заданными вероятностями и не официальные результаты. Исследовательская организация может вести реестр будущих прогнозов, если определит измеримое событие, дату разрешения, источник результата и правило вероятности, не датируя выпуск задним числом.

11. Научные ограничения: где заканчивается право этого исследования на утверждение?

- 1. Измерение:** статья не содержит данных об услугах Саудовской Аравии, их доступности, распределении полномочий, инцидентах или применимости к ним законов. Результаты примера с синтетическим числом три нельзя переносить на реальные суммы или реестры.
- 2. Вычисления:** полностью исследованы 25 состояний спроса, а не пространство состояний реальных систем с тысячами ролей, ключей, устройств, отзывов, случаев принуждения и человеческих ошибок.
- 3. Безопасность:** модель не доказывает устойчивость оборудования, ключей, сообщений или платёжных способов к взлому; пример копируемого жетона специально показывает ограниченность действительности подписи.
- 4. Социальное представление:** каждое состояние примера — всего два числа. Различия возможностей людей, важность действия, права на обжалование и возмещение не включены в модель и фигурируют только как требования к предлагаемому исследованию.

5. **Исторический материал:** ни случай на Пиренейском полуострове, ни случай Британской библиотеки нельзя превратить в доказательство качества конкретной локальной архитектуры. Источники фиксируют сбои услуг или сохранение их частей, но не измеряют действие предложенного «профиля полномочий».
6. **Предвзятость:** остановка и предварительный приём включены как реальные альтернативы, а слепая политика намеренно сконструирована как контрпример. Поэтому сравнение не претендует на нейтральность между внедрёнными коммерческими решениями.
7. **Правомерность:** полномочия людей и учреждений определяются правом и управлением; экспериментальная модель не вправе выдавать разрешения вместо уполномоченной инстанции. Определение допустимых действий предшествует техническому исследованию их пределов.

12. Следующее решающее исследование

Самый полезный следующий шаг — не огромная платформа, объявленная способной работать без интернета, а выбор **одного публичного действия**, которое законно принимать предварительно; второго, которое при разрешающей политике можно завершить в пределах действительной выделенной доли; и третьего, которое должно остановиться. В санкционированной испытательной среде с явными юридическими результатами измеряется, что произошло с запросом, свидетельством, правом и заявителем **во время отключения и после восстановления связи**.

Решающей станет статья, способная сказать: при конкретных видах отключения и названных условиях архитектура (X) увеличила число корректно завершённых действий по сравнению с политикой (Y), не нарушив утверждённых инвариантов; её стоимость и социальные пределы были такими-то. Результатом может стать неудача предложенной архитектуры или превосходство более простого варианта. Готовность принять такой результат — часть исследовательского метода, а не редакционное неудобство, которое следует скрывать.

13. Воспроизводимость, источники и данные

Повторный запуск: сохраните файлы каталога, установите зависимости из `analysis/requirements.txt` и выполните:

```
python3 analysis/reproduce.py
```

Программа заново создаст `data/model_check_states.csv`, `data/model_check_summary.csv`, `data/model_assumptions.json`, `data/duplicate_token_counterexample.json` и два рисунка в форматах SVG и PNG. Код и синтетические данные полностью находятся в пакете и не зависят от закрытых рабочих наборов данных или ключей доступа.

Доступность источников о реальных событиях: статьи и опубликованные отчёты представлены ссылками на учреждения и исследователей, которым они принадлежат. Мы не распространяем заново защищённые ими файлы и не заявляем о лицензии на исходные банковские данные. Реестр источников фиксирует состояние доступа во время подготовки исходного пакета; это историческая запись аудита, а не описание действующего ограничения на извлечение текста из документов. Все числовые значения модели основаны на объявленных в коде синтетических переменных.

Документированные источники в порядке цитирования

1. **S01** Banco de España. *How do we pay when the power goes out? Spain's blackout experience*. 27 April 2026. Original institutional blog. <https://www.bde.es/wbe/en/noticias-eventos/blog/como-pagamos-cuando-todo-se-apaga-la-experiencia-del-apagon-en-espana.html>
2. **S02** European Central Bank. *Keep calm and carry cash: lessons on the unique role of physical currency across four crises*. ECB Economic Bulletin, 2025. https://www.ecb.europa.eu/press/economic-bulletin/articles/2025/html/ecb.ebart202506_02~1a773e2ca3.en.html
3. **S03** ENTSO-E. *Final report of the expert panel on the blackout in Spain and Portugal*. Published 20 March 2026. <https://www.entsoe.eu/news/2026/03/20/entso-e-publishes-expert-panel-final-report-on-28-april-2025-blackout-in-spain-and-portugal/>
4. **S04** CaixaBank Research, Josep Mestres Domènech and Zoel Martín Vilató. *The economic impact of the blackout in detail*. 18 June 2025. <https://www.caixabankresearch.com/en/sectoral-analysis/consumption/economic-impact-blackout-detail>
5. **S05** Banco de España. *Situation of payment infrastructures and the banking sector in Spain after the blackout*. 29 April 2025. <https://www.bde.es/wbe/en/inicio/noticias/monitorizacion-del-impacto-del-apagon-el-sistema-financiero.html>
6. **S06** BIS Innovation Hub. *Project Polaris: handbook for offline payments with CBDC*. 11 May 2023. <https://www.bis.org/publications/project-polaris-handbook-offline-payments-cbdc>
7. **S07** BIS Innovation Hub. *Project Polaris: high-level design guide for offline payments*. 26 October 2023. <https://www.bis.org/publications/project-polaris-high-level-design-guide-offline-payments>
8. **S08** Joseph M. Hellerstein and Peter Alvaro. *Keeping CALM: When Distributed Consistency is Easy*. Author-hosted 2019 preprint; subsequent publication context noted separately in source ledger. <https://arxiv.org/html/1901.01930v2>
9. **S09** Peter Bailis and collaborators. *Coordination Avoidance in Database Systems*. Proceedings of the VLDB Endowment, volume 8, 2014. <https://www.vldb.org/pvldb/vol8/p185-bailis.pdf>
10. **S10** Marc Shapiro, Nuno Preguiça, Carlos Baquero and Marek Zawirski. *Conflict-Free Replicated Data Types*. SSS 2011, LNCS 6976. DOI: 10.1007/978-3-642-24550-3_29. <https://inria.hal.science/inria-00609399v2/document>

11. **S11** Digital Government Authority. *Controls of Risk and Business Continuity Management for Digital Government, V2.0; Guideline of Risk and Business Continuity Management for Digital Government, V1.0* (2025). <https://dga.gov.sa/sites/default/files/2024-02/Controls%20Of%20Risk%20and%20Business%20Continuity%20Management%20For%20Digital%20Government%20V2.0.pdf>
12. **S12** Saudi Central Bank. *Business Continuity Management Framework*, introduction, 27 February 2017, in force. <https://rulebook.sama.gov.sa/en/11-introduction-bcm-framework>
13. **S13** Saudi Central Bank. *Providing Backup Generators in Branches and Remittance Centers*, circular of 18 May 2021. <https://rulebook.sama.gov.sa/en/providing-backup-generators-branches-and-remittance-centers>
14. **S14** British Library. *British Library Cyber Incident Review*. 8 March 2024, primary post-incident account. <https://www.bl.uk/files/v5dwkion/production/99206a2d1e9f07b35712b78f7d75fbb09560c08d.pdf/british-library-cyber-incident-review-8-march-2024.pdf?dl=>
15. **S15** British Library. *Restoring our services – November 2025 update*. 21 November 2025. <https://www.bl.uk/stories/news/restoring-our-services-november-2025-update>
16. **S16** European Central Bank. *Call for expression of interest to provide feedback on the list of standards relevant for the offline digital euro*. 18 August 2026. <https://www.ecb.europa.eu/press/intro/news/html/ecb.mipnews260818.en.html>
17. **S17** European Central Bank. *FAQs on the digital euro*. Updated 17 August 2026; conditions for development, legislation and potential 2029 issuance. https://www.ecb.europa.eu/euro/digital_euro/faqs/html/ecb.faq_digital_euro.en.html