Блокчейн-технологии цифровой экономики

в рамках дисциплины

Теоретическая инноватика

Надежда Николаевна Покровская
Кандидат экономических наук, доктор социологических наук, профессор
Профессор кафедры международного бизнеса СПбГЭУ

Nadezhda N. Pokrovskaia
PhD in Economics, Doctor in Sociology, professor
International School of Economics and Politics,
Saint-Petersburg State University of Economics

Блокчейн-технологии в цифровой экономике

- Децентрализованные (распределенные) регулятивные механизмы и реплицированный реестр
  - Суть
  - Актуальность
- Экономика знаний
- Цифровая экономика
- Принципы блокчейн-технологии
- Применение блокчейн-технологий в цифровой экономике

Social vs Technical Regulation
or
Social + Technical Regulation

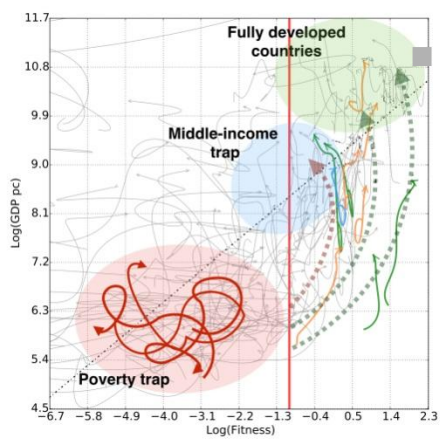
- Санкт-Петербург – интеллектуальная столица России
- Петр I основал Санкт-Петербург в
  - 1708
  - 1703
    - Блокчейн – реплицированный распределенный реестр (база данных)
      не подтверждающий ошибочных утверждений
    - непрерывно растущая глобальная цепочка блоков с записями обо всех транзакциях

Российские банки планировали применять Реестр Мастерчейн в середине 2018

- 5 октября 2016
  - Банк России разработал и протестировал прототип блокчейн платформы ‘Masterchain’
    - Распределенный реестр
    - На основе Ethereum
    - VTB Group, Sberbank PJSC, Alfa Bank, Tinkoff Bank,
    - Qiwi Group, национальная система платежных карт НСПК
- Июнь 2017
  - В.В. Путин встретил автора Ethereum - Vitalik Buterin
- Лето 2017
  - Внешэкономбанк запустил электронный кошелек для благотворительного фонда «Старость в радость» и провел первую транзакцию в криптовалюте Ether (эфир)
- Середина 2018
  - планы внедрить Masterchain как общую платформу
    - Институциональная ловушка ?

Контекст:
IT и экономика знаний

- Глобальная экономика знаний
  - Инфраструктура
  - Прозрачность ИКТ
  - Мобильность ресурсов
- Экономика знаний
  - High-road competition
    - конкуренция за инвестиции и человеческий капитал
    - Зависимость от ICT-сектора (пример Финляндии)
    - Middle-income trap – и роль высшего образования
      - http://www.nber.org/papers/w18673.pdf
      - http://voxeu.org/article/growth-slowdowns-redux-avoiding-middle-income-trap



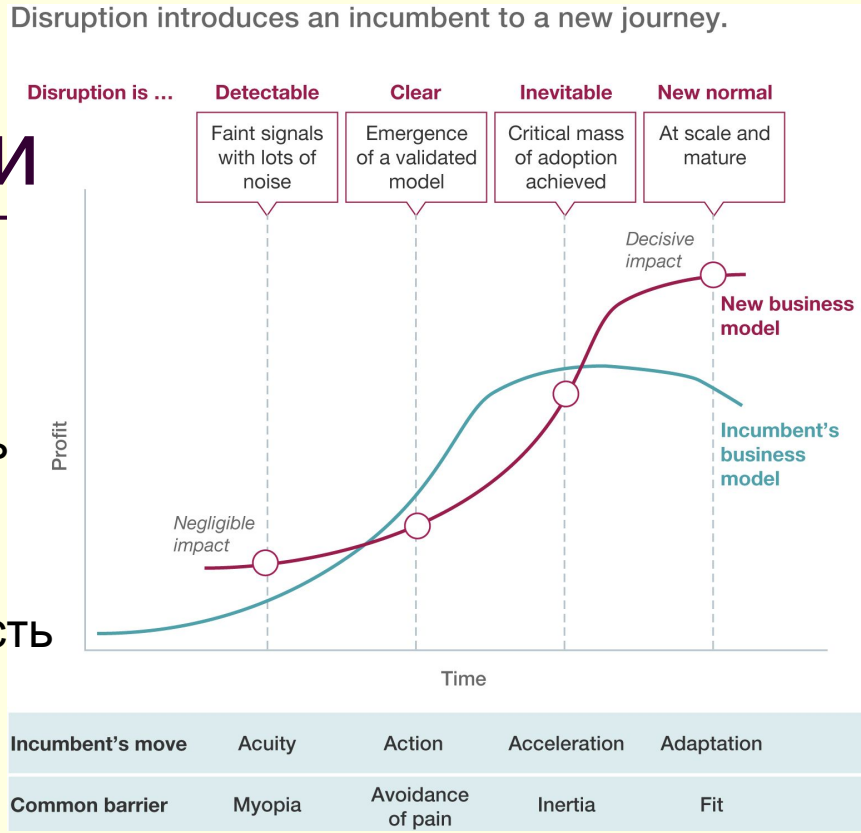
- Информация и коммуникации
  - Объективизация виртуальной реальности
    - Augmented reality
  - Сжатие пространства и времени
  - Коммуникативные технологии и компетенции

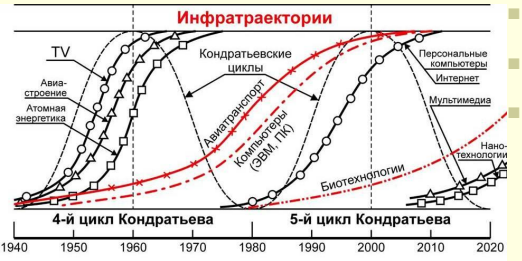
NOKIA
Connecting People

Nokia Lumia
Connecting people first.

Контекст: управление знаниями

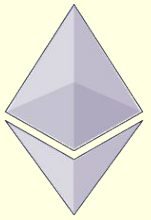
- Инновационный рост – disruption
  - Частная инициатива
  - Кластеры – среда знаний
  - Личное знание, компетентность
- Производство, передача знаний
  - Безопасность
  - Интеллектуальная собственность
- Потребление знаний
  - Коммерциализация ИС
- Государственные институты
  - Среда – социокультурные регуляторы поведения
    - Система ценностей и социальных установок
- Бизнес-инфраструктура и цифровая экономика
  - Agile-менеджмент, Lean start-up, MVP – minimum viable product
  - Агрегаторы
  - Умная среда, умные устройства
  - IoT, Internet of Everything, connected factories (Industry 4.0)





Контекст: цифровая экономика знаний

- Технологии цифровой экономики
  - экономико-управленческие
    - Уберизация
      - We-economy, sharing economy
    - кастомизация и индивидуализация производства, вплоть до 3D-printing
      - Приближение к месту потребления, логистика сырья
  - вычислительные – Cloud & Fog computing
    - транзакции – Internet of things, Internet of Everything
  - регулятивные
    - геймификация, креативизация
  - Децентрализация и прозрачность
    - Blockchain (налоги – 2023)
    - Etherium (контракты)



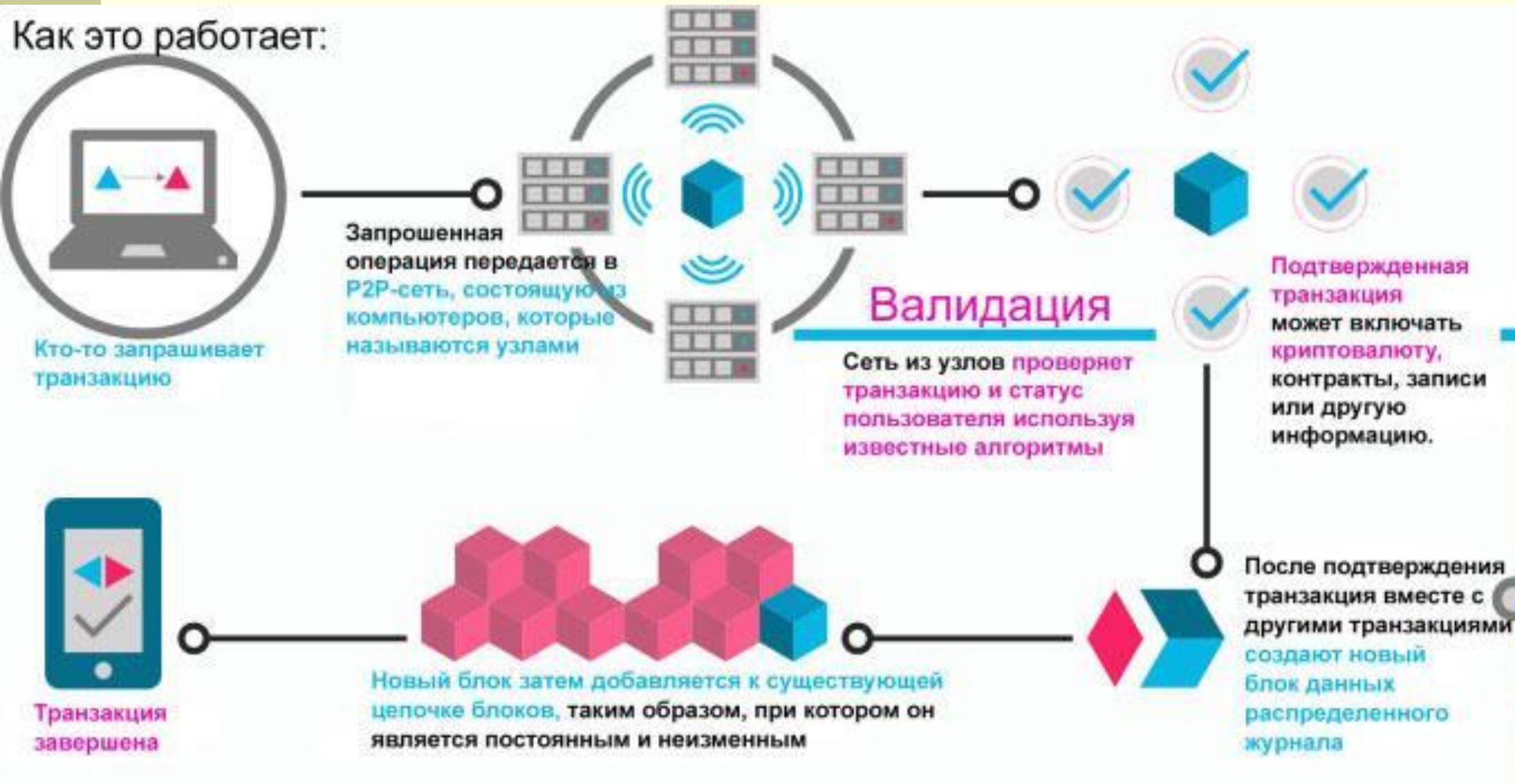
Базовые проблемы, которые привели к успеху блокчейна

- Кибер-преступность
  - Использование кредитных карт
- «Пузырь» цен на недвижимость
  - Кризис 2007-2009
- Паника и крах биржи
  - Инвестировать в dot com ?
- Коллапс страховых и банковских институтов
  - Создание местных денег
- Нехватка доверия прозрачному рынку
  - Традиционные феодальные семейные типы организации потоков ресурсов

Распределённая база данных

- Безопасность в технологии блокчейн обеспечивается через децентрализованный сервер и одноранговые (P2P, пиринговые – peer-to-peer) сетевые соединения
- При новой записи проставляются метки времени
- Формируется реестр («цепь»), управляемая автономно
- Реплицированная распределённая база данных
  (Distributed ledger technologies, DLTs)
  - таблица, миллионы раз продублированная в компьютерной сети
    - Октябрь 2017 – в системе биткойна работало 375 тыс. человек
  - информация в блокчейне существует как общая, публичная и постоянно сверяемая база данных
  - ее копии хранятся на всех компьютерах сети
- сеть разработана так, что она регулярно обновляет эту таблицу
- удобно для:
  - регистрации событий
    - внесения медицинских записей,
    - прав собственности на акции, недвижимость…
  - операций с данными
  - управления идентификацией (например, гражданство) и подтверждения подлинности источника

Механизм блокчейн



- Пользователи могут изменять только те части цепочки блоков, которыми они «владеют» - у них есть закрытые ключи, без которых запись в файл невозможна
- Шифрование гарантирует синхронизацию копий распределенной цепочки блоков у всех пользователей

https://mining-cryptocurrency.ru/blockchain/

Одноранговая сеть - преимущества

- Можно проверить состояние блокчейна, используя программу-проводник (*blockchain explorer*)
- Не надо полагаться только на одну сторону, чтобы знать истинное состояние блокчейна.
- Не надо полагаться на безопасность одного сервера, чтобы знать, что блокчейн защищен
- Злоумышленнику придется одновременно взломать тысячи компьютеров, а не один сервер.
- Всегда есть уверенность, что блокчейн никогда не исчезнет, потому что для этого его надо будет уничтожить всем узлам

- Как узнать, что все транзакции в блокчейне верны?
- Как узнать, что в блоках нет недействительных транзакций?
- если есть разные версии blockchain, как узнать, которые из них (ветвей) являются истинными?

Верификация: ключи

- https://www.pwc.ru/ru/publications/blockchain/blockchain_opportunity-for-energy-producers%20and-consumers_RUS.pdf

Верификация и консенсус

- Цель процесса верификации – добиться консенсуса по информации, содержащейся в распределенном реестре
- Верификация на основе консенсуса – децентрализованный процесс, встроенный в саму цепочку блоков и автоматизированный:
  - Доказательство выполнения работы
    - на основе майнинга
  - Подтверждение доли

Верификация – доказательство выполненной работы

- Алгоритмы верификации данных в каждом блоке присваивают каждому блоку уникальный хеш-код на основе хранящейся в нем информации
  - Хеш-коды - обычные или криптографические хеш-комбинации
  - конкретный хеш-код идентифицирует информацию, которая содержится в блоке
  - Уровень сложности корректируется с учетом вычислительной мощности в сети майнеров, чтобы хеширование новых блоков происходило с установленной периодичностью (Биткойн: 10 минут; Эфириум: 10 сек.)
- если информация по операции впоследствии меняется (несанкционированное вмешательство, ошибки передачи данных…), применяемый к блоку алгоритм не будет генерировать правильный хеш-код
- Хеш-коды, рассчитанные для того же блока, который был сохранен несколько раз в децентрализованной сети, сопоставляются так, чтобы выявить измененные блоки и объявить их недействительными
- Верифицированная правильная версия блока выявляется большинством участвующих компьютеров и добавляется к другим, ранее верифицированным блокам, удлиняя цепочку блоков
- Когда блок, содержащий первоначальную операцию, добавляется к цепочке блоков и данное добавочное звено сохраняется достаточным количеством участников сети, операция подтверждается, о чем информируют обе стороны сделки

Механизм консенсуса и 51%

- Распределенные реестры являются точными копиями на тысячах вычислительных устройств (компьютеров, смартфонов…)
  - снижает риск появления мошеннических транзакций
- Криптографические алгоритмы хеширования гарантируют, что любое изменение входных данных транзакции приведет к появлению другого значения хеша в результатах расчетов, что указывает на вероятность компрометации входных данных транзакции
- Электронно-цифровые подписи гарантируют, что транзакции осуществляются легитимными отправителями (подписаны закрытыми ключами), а не злоумышленниками
- Децентрализованная одноранговая блокчейн-сеть лишает отдельных участников или групп участников возможности контролировать базовую инфраструктуру или дестабилизировать всю систему
  - Исключение – ассоциативное владение >50% сети
- По сути система записывает хронологический порядок проведения транзакций со всеми узлами сети, признавшими действительность транзакций посредством выбранной модели консенсуса
- Результатом являются не подлежащие отмене транзакции, согласованные всеми участниками сети децентрализованно

Децентрализация управления

- Блокчейн – защищенный от несанкционированного доступа цифровой реестр общего пользования, который ведет учет транзакций в публичной или закрытой одноранговой сети.
- Распределенный между всеми узлами сети реестр непрерывно записывает историю операций с активами между одноранговыми (одного порядка) узлами сети в виде блоков информации
- Все утвержденные блоки транзакций соединяются в цепочку — с начального блока до последнего добавленного
  - block chain – цепочка блоков
- блокчейн выступает в качестве единого источника достоверных данных, а участники блокчейн-цепи видят только те транзакции, которые относятся именно к ним
- Вместо того, чтобы обращаться к посредникам при проведении транзакций, узлы блокчейн-сети используют специальный протокол консенсуса для согласования содержимого реестра, а также криптографические алгоритмы хеширования и электронно-цифровые подписи для обеспечения целостности транзакции и передачи ее параметров

Интернет ценностей - IoV

- Каждый человек может разместить в Интернете информацию, другие могут получить к ней доступ
- Цепочки блоков позволяют отправлять любые ценности, которые могут быть оцифрованы – например, право собственности на акции или на недвижимость
- Пользователь получает закрытый ключ, созданный по криптографическому алгоритму, который разрешает доступ только к тем блокам, которыми он «владеет»
- Предоставляя кому-либо закрытый ключ, пользователь передает ту ценность, которая хранится в соответствующем разделе цепочки блоков.
- доверие опирается на подтверждение подлинности личности – никто не может изменять цепочку блоков без соответствующих ключей, которые обеспечиваются метками времени и хешами (итоговыми строками) во всех узлах

Блокчейн 1.0 – bitcoin

- виртуальные валюты (криптовалюты)
  - Биткойн…
- используются в качестве альтернативы реальным (фиатным) валютам

- Все участники сети равны и подключаются к ней по одинаковому протоколу
- Участники – физические лица, государственные структуры, организации или объединения всех перечисленных типов участников

Блокчейн 2.0 – smart contracts

- модели «умных контрактов»
- Умный контракт - цифровой протокол, автоматически исполняющий заранее предопределенные процессы транзакции и не требующий участия третьей стороны (например, банка)
- создание полностью автоматизированного «умного контракта» между производителем электроэнергии и потребителем, который будет регулировать в автономном и защищенном режиме как поставки, так и платежи
  - если покупатель, например, не сможет осуществить платеж, «умный контракт» автоматически приостановит электроснабжение до получения платежа, при условии что стороны заранее договорились о включении такого механизма в свой контракт

Anjum A., Sporny M., Sill A. Blockchain Standards for Compliance and TrustArticle // IEEE Cloud Computing 4(4):84-90 · July 2017
https://www.researchgate.net/publication/320364955_Blockchain_Standards_for_Compliance_and_Trust

Performance Characteristics of Blockchains

Principle	Bitcoin	Ethereum	Stellar	IPFS	Blockstack	Hashgraph
Consistency	Block verifications. 30–60 minutes	Block verifications. 20–60 minutes	Single block verification. Less then 1 minute	P2P mirroring. Limited primarily by network I/O. Several seconds for files less than 128KB.	Block verifications. 30–60 minutes	Consensus with probability one; Byzantine agreement, but attackers must control less than one-third
System Availability	Block verifications. 30–60 minutes	Block verifications. 20–60 minutes	Single block verification. Less then 1 minute	Single storage request response. Several seconds for files less than 128KB.	Block verifications. 30–60 minutes	Virtual voting; DoS resistant without proof-of-work, fast gossip
Failure Tolerance	Longest chain wins	Longest chain wins	Last balloted block always has consensus.	Content address hash. Highly resilient against network partitioning	Longest chain wins	Strong Byzantine fault tolerance

Anjum A., Sporny M., Sill A. Blockchain Standards for Compliance and TrustArticle // IEEE Cloud Computing 4(4):84-90 · July 2017
https://www.researchgate.net/publication/320364955_Blockchain_Standards_for_Compliance_and_Trust

Scalability	Block size. 7 transactions per second	Block size. 7–20 transactions per second	Thousands to tens of thousands of transactions per second.	Thousands to tens of thousands of transactions per seconds. Scales linearly as nodes are added.	Block size. 7 transactions per second	Thousands to tens of thousands of transactions per seconds. Limited by bandwidth only
Latency	Block verifications. 30–60 minutes	Block verifications. 20–60 minutes	Single block verification. Less than 1 minute.	Single storage request response. Several seconds for files less than 128KB.	Block verifications. 30–60 minutes	Virtual voting; limited only by exponentially fast gossip protocol
Auditability	Full	Full	Full	Difficult	Full	Configurable
Liveliness	Full	Full	Full	Fails if nodes storing data fail	Full	Full
Denial of Service Resistance	Spend Bitcoin	Spend Ether	Spend Stellar	Files are only mirrored if requested	Spend Bitcoin	Signed State/ Proof-of-stake/ <1/3 attackers
System Complexity	Medium	High	Medium	Medium	Medium High	Low, but not full system

Many Different Types of Blockchains

https://www.researchgate.net/publication/320364955_Blockchain_Standards_for_Compliance_and_Trust

Principle	Bitcoin	Ethereum	Stellar	IPFS	Blockstack	Hashgraph
Confidentiality	None	None	None	Hash-based content addresses	None	None
Information availability	Block mirroring	Block mirroring	Ledger mirroring	Graph and file mirroring	Block mirroring/ DHT mirroring	Hashgraph/ mirroring; Optional Event History
Integrity	Multiple block verifications	Multiple block verifications	Latest block verification	Hash-based content addressing	Multiple block verifications	Consensus with probability one
Non repudiation	Digital signatures	Digital signatures	Digital signatures	Digital signatures	Digital signatures	Digital signatures
Provenance	Transaction inputs/outputs	Ethereum state machine and transition functions	Digitaly signed ledger transition instructions	Digital signatures and versioning	Transaction inputs & outputs and virtual chain references	Hashgraph/ mirroring; Optional Event History
Pseudonymity	Public keys	Public keys and contract addresses	Public keys	Public keys	Public keys, but public information encouraged	Not supported; could be layered
Selective disclosure	None	None	None	None	Selective access to encrypted storage	Not supported; could be layered

Блокчейн 3.0 - концепция

- этап развития технологии
- проработка концепции «умного контракта»
- Цель – создание децентрализованных, автономных организационных единиц, которые руководствуются собственными законами и действуют, по сути, автономно

Блокчейн – закрытые цепочки

- Открытая цепочка блоков
  - сохраняется анонимность всех участников системы
  - Пример – платформы «Биткойн» и «Эфириум»
- В закрытых блокчейн-системах все участники известны и идентифицированы до того, как будет предоставлен доступ

  Преимущества:
  - позволяют использовать более простые структуры корпоративного управления и стоимость обслуживания ниже, чем у открытых
  - банки и поставщики платежных услуг в рамках своих текущих бизнес-моделей могут в некоторой степени сохранить контроль и потенциал генерирования выручки

Australia' Survey results (Dec 2016):

Blockchain use' cases – potential applications in finances, management, government services

Government services that survey respondents would like to see using blockchain technologies to improve efficiencies and public access

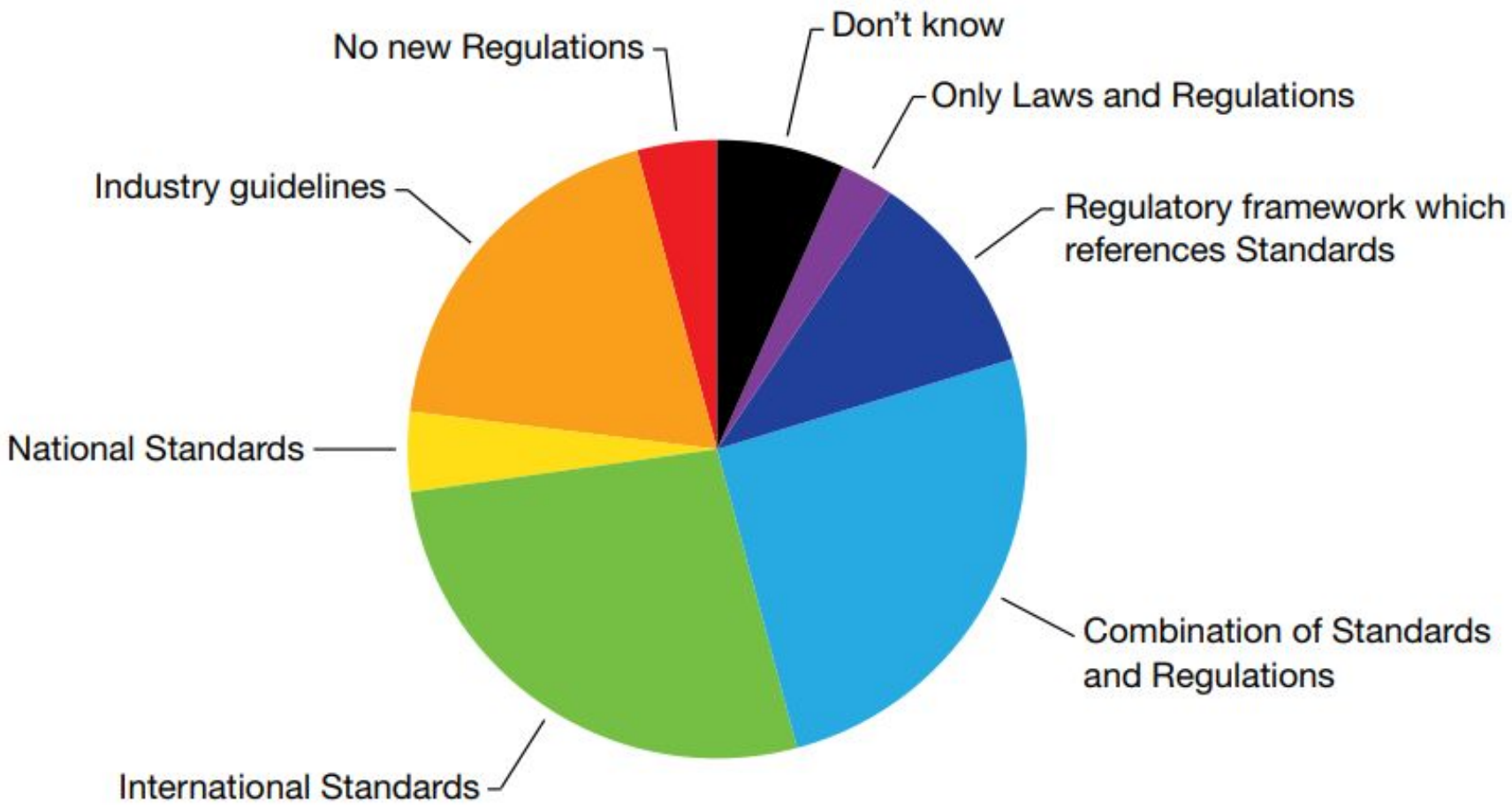
Land Transfers and Property Title registrations	72.1%
Personal Identification and Passport Documentation	68.9%
Management of Health Records	65.6%
Vehicle Registrations	54.1%
Welfare Distribution and Monitoring	37.7%
Urban planning; wider pedestrian sidewalks, increased times for crossings	21.3%
Public Transport Scheduling	16.4%

Source: Blockchain survey, Standards Australia analysis

Australia' Survey results :

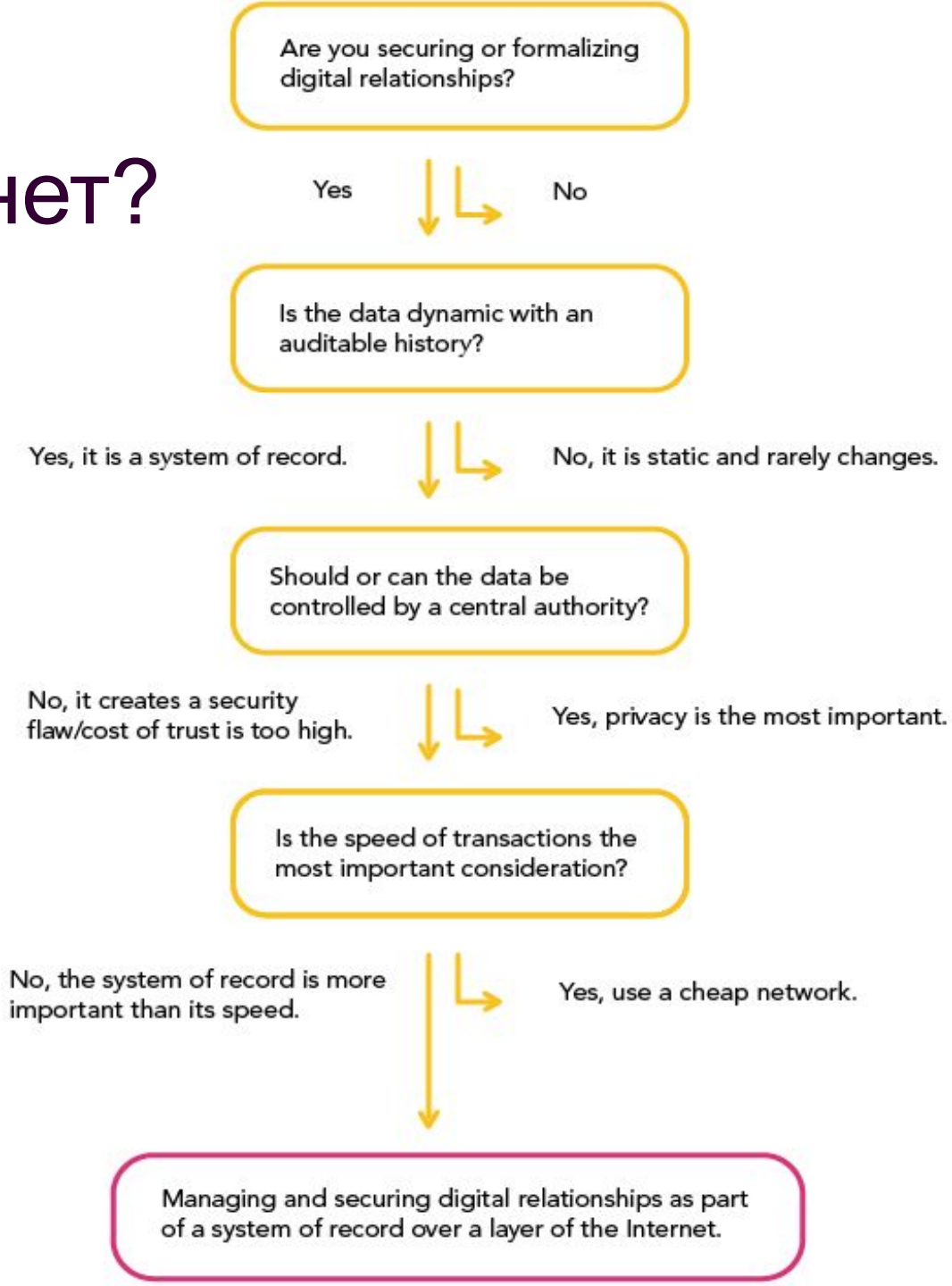
the roll out of blockchain technologies

The optimum standards and regulatory framework to ensure we are fostering innovation and entrepreneurism



More than 88% of respondents indicate a role for standards in supporting the roll out of blockchain technologies. Source: Blockchain survey, Standards Australia analysis

Схема выбора Блокчейн или нет?



Мастерчейн – история

- ЦБ РФ, Сбербанк, ВТБ, Газпромбанк, Райффайзен банк, «РНКО платежный центр», и др. создали Российскую Ассоциацию «Финансовые технологии»
- Тестовые операции в системе Мастерчейн совершены в октябре 2016 г.

- Masterchain – доверенная среда обмена информацией и управляющими воздействиями между не доверяющими друг другу сторонами
- нацелена на снижение участия посредников взаимодействий, доступность информации для заинтересованных сторон в момент внесения изменений, контролируемую передачу прав собственности на финансовые инструменты и активы с выполнением соответствующего учета

Криптовалюты как мера вещей?

- A virtual currency known as “gas” will be used for validating transactions within Masterchain
- Ether (“Gas”) is an abstract unit measurement for the resources needed to process one transaction and record it to the distributed ledger
- Masterchain will require computing capacity in order to validate transactions.
- Russia’s central bank has already implemented an Ethereum-based blockchain for processing online payments and verifying customer data with lenders.

Стандарты и сертификаты

- Использование платформ Ethereum, Hyperledger не предполагает хранения персональных данных
- Masterchain построен на платформе Ethereum
  - Но не соединяется с существующими узлами публичных протоколов
- ISO/TC 307 - Blockchain and distributed ledger technologies (Creation date: 2016)
  - https://www.iso.org/committee/6266604.html
- ISO/IEC JTC 1/SC 38 Cloud Computing and Distributed Platforms
  - https://www.iso.org/committee/601355.html
- Australia' Road map for Blockchain standards
  - https://www.standards.org.au/StandardAU/Media/SA-Archive/OurOrganisation/News/Documents/Roadmap_for_Blockchain_Standards_report.pdf

Примеры использования

- http://masterchain.rbc.ru/

- Знать своего потребителя – know your customer (KYC)
- Регистрация кадастра (недвижимость)
  - (UK – April 2017 – “Digital Street”)
- Банковские гарантии
- Цифровые аккредитивы
- Рынок труда
  - Дипломы, сертификаты, резюме и вакансии

Мастерчейн – как Реестр прав собственности на недвижимость

Внедрение национальных платформ для регистрации прав

- Ведение и регистрация прав собственности:
  - Швеция, ОАЭ, Индия
  - В феврале 2017 г. Национальное агентство публичного реестра Грузии и поставщик блокчейн-решений Bitfury подписали меморандум, в рамках которого в стране начнет внедряться основанный на новой технологии сервис, регистрирующий права собственности. Сервис позволит заменить нотариальное оформление документов регистрацией актов продажи и покупки участков в системе
  - В апреле 2017 г. Земельный реестр Великобритании обнародовал детали инициативы Digital Street, которая должна упростить процедуру регистрации купли-продажи земельных участков и объектов недвижимости

- Электронное гражданство на блокчейн
  - Финляндия, Эстония, Бразилия

Цифровизация и Министерство

- Цифровизация экономики сегодня провозглашена на уровне Президента РФ и председателя правительства, а также закреплена в документах:
- - Программа "Цифровая экономика Российской Федерации», утв. распоряжением Правительства РФ от 28 июля 2017 г. № 1632-рм
- - Доктрина информационной безопасности РФ, утв. Указом Президента РФ от 5 декабря 2016 г. № 646
- - Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы, утв. Указом Президента РФ от 9 мая 2017 г. № 203

Masterchain для индивидуализации портфолио

- Накопление документов, сертификатов
  - Возможность ввода данных
    - Документы
      - Подтверждение от учреждений
    - Личные интересы, достижения, предпочтения
- Оперативный ввод вакансий работодателями
  - Описание требуемого функционала
  - Сравнение
    - Со стандартами
      - Профессиональные стандарты – ФГОС ВО
    - С личными интересами, результатами
- Работодатель «собирает» функционал под свою потребность (лего)

Внедрение национальных платформ для регистрации прав

- Попытки применять блокчейн для решения задач ведения и регистрации прав предпринимаются в ряде стран

- В феврале 2017 г. Национальное агентство публичного реестра Грузии и поставщик блокчейн-решений Bitfury подписали меморандум, в рамках которого в стране начнет внедряться основанный на новой технологии сервис, регистрирующий права собственности. Сервис позволит заменить нотариальное оформление документов регистрацией актов продажи и покупки участков в системе

- В апреле 2017 г. Земельный реестр Великобритании обнародовал детали инициативы Digital Street, которая должна упростить процедуру регистрации купли-продажи земельных участков и объектов недвижимости

Спасибо за внимание

Пожалуйста, Ваши вопросы?

Покровская Надежда Николаевна
nnp@europe.com