

# Initial Coin Offering (ICO)

19 декабря 2017

# Резюме

- **Объем привлеченных средств через ICO приближается к 4 млрд долларов США** и превышает объем венчурного инвестирования в блокчейн-проекты почти в два раза. С осени 2017 года объем привлечений начал замедляться, все меньше проектов достигают цели по сбору средств.
- **Объект ICO инвестирования – токен**, в большинстве случаев, средство оплаты услуг на блокчейн-платформе. На момент ICO эта платформа, как правило, отсутствует, а токен содержит минимум обязательств эмитента.
- **Необходимость блокчейна и собственного токена в ICO проектах часто не оправдана.** Пока основной успех проектов на открытом блокчейне приходится на проекты в финансовой сфере и на платформы для создания других блокчейн-проектов. Самый успешный проект – это Ethereum, его основное применение - ICO.
- **Большинство ICO используют платформу Ethereum.** Сеть перегружена, рост стоимости Ether ведет к росту стоимости ICO. Условия и функционал токена формулируются в смарт-контракте – программном коде, который может содержать ошибки или преднамеренные «закладки».
- **Оценка определяется ажиотажем ICO и больше похожа на оценку золота**, хотя должна определяться прогнозами развития проекта и природой токена. Это приводит к экстремальной волатильности при последующих торгах токена на бирже.
- **Объемы ICO вызывают всплеск интереса хакеров**, более 10% средств от ICO теряются в результате атак. Кроме потери средств проект рискует репутацией, а инвесторы персональными данными.
- **Большинство регуляторов двигаются от игнорирования ICO до его запрета или регулирования в соответствии с природой токена.** Игроки рынка вырабатывают собственные принципы, один из наиболее интересных - SAFT.
- **Общий настрой в РФ: блокчейн хорошо, биткоин нет, ICO надо регулировать как IPO.** Но в соответствии с действующим законодательством рубль - это единственный инструмент расчета, а создание валютных суррогатов запрещено.
- **Будущее ICO:** сейчас ICO стал синонимом ажиотажа и очень высокого риска. Однако эта форма краудфандинга дает уникальные возможности: если с помощью блокчейн-функционала решается существующая проблема, собственный токен действительно необходим, а дополнительное финансирование и активное участие инвесторов улучшает проект. С точки же зрения защиты интересов всех участников ICO прозрачность открытого блокчейн пока недостаточно используется, и здесь есть возможности для регуляторов, самих проектов и инвесторов.

1. Статус рынка ICO
2. Применение открытого блокчейна и ICO
3. Выбор платформы и смарт-контракт
4. Оценка токена
5. Безопасность
6. Регулирование
7. Что делать
8. Приложения

- 1. Статус рынка ICO**
2. Применение открытого блокчейна и ICO
3. Выбор платформы и смарт-контракт
4. Оценка токена
5. Безопасность
6. Регулирование
7. Что делать
8. Приложения

Всего проанализировано проектов

**372**

Детальный анализ по проектам

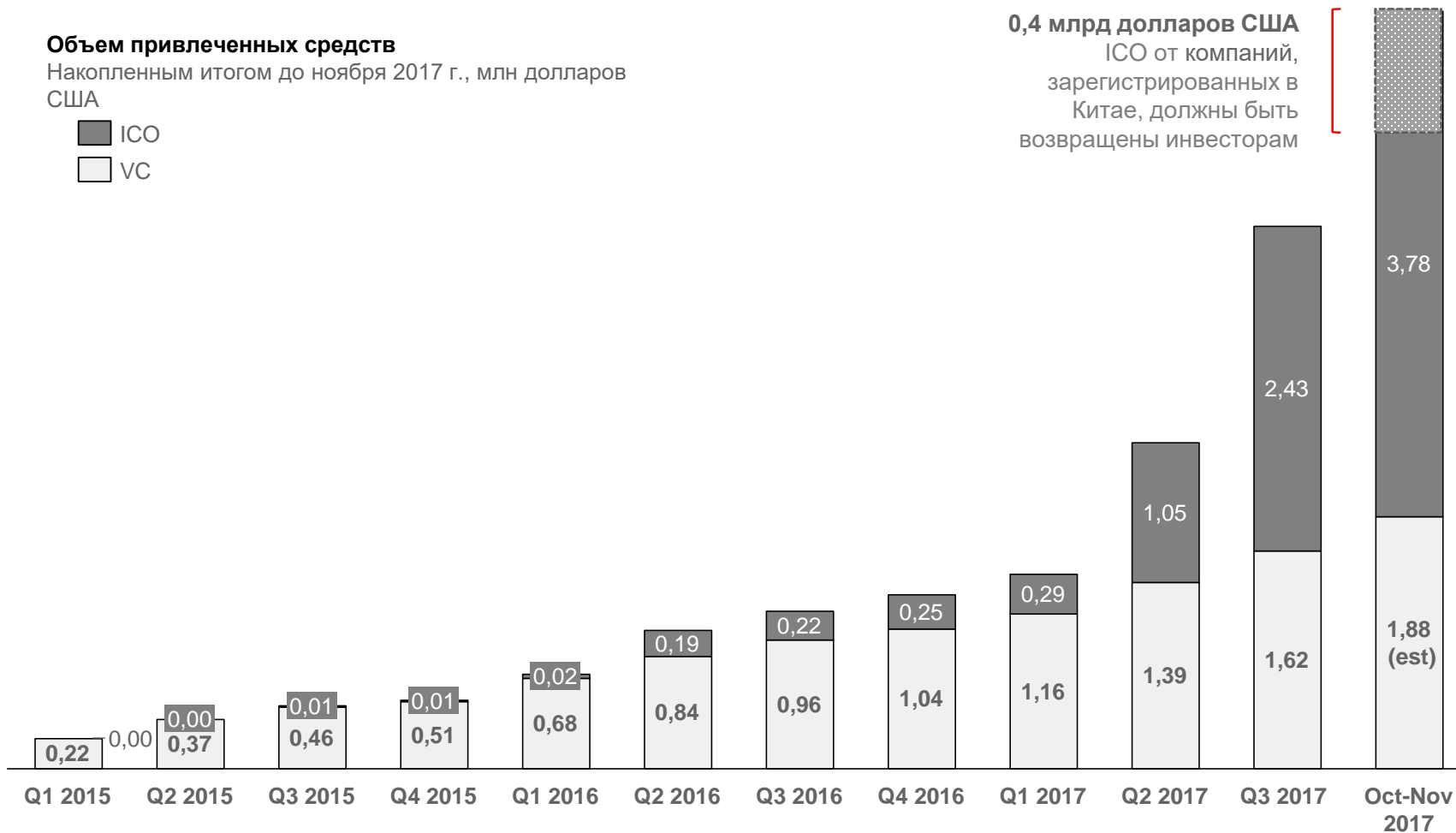
**110**  
(87% от сборов)

# Статус рынка ICO

## Общий объем средств, собранных при ICO, превысил 3,7 млрд долларов США и обогнал объемы венчурного инвестирования

### Объем привлеченных средств

Накопленным итогом до ноября 2017 г., млн долларов США

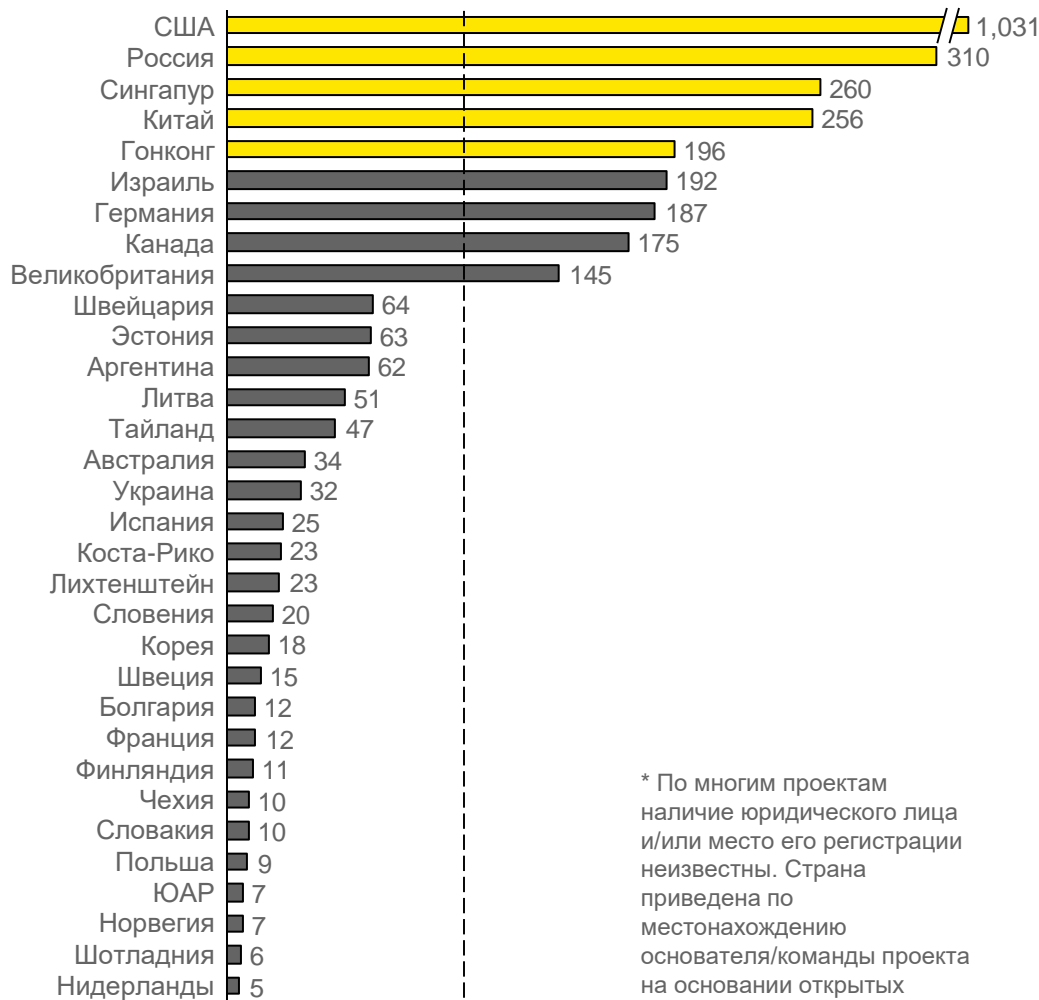


0,4 млрд долларов США  
ICO от компаний,  
зарегистрированных в  
Китае, должны быть  
возвращены инвесторам

Примерные данные на основании открытых источников - рынок ICO не регулируется, отсутствует стандартизированная отчетность, существует множество платформ, характерна большая волатильность.

## Российские проекты входят в тройку лидеров по объемам сборов

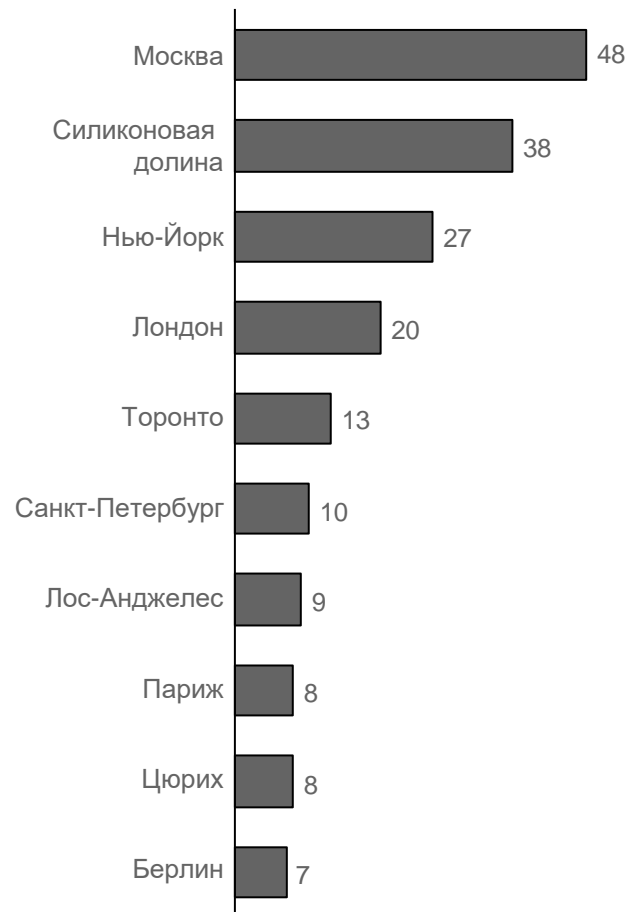
Сборы ICO по странам\*, млн долларов США <sup>(1)</sup>



\* По многим проектам наличие юридического лица и/или место его регистрации неизвестны. Страна приведена по местонахождению основателя/команды проекта на основании открытых источников

Ø 104

Топ-10 городов по количеству проектов ICO, основанных на местонахождении CEO/основателя <sup>(2)</sup>



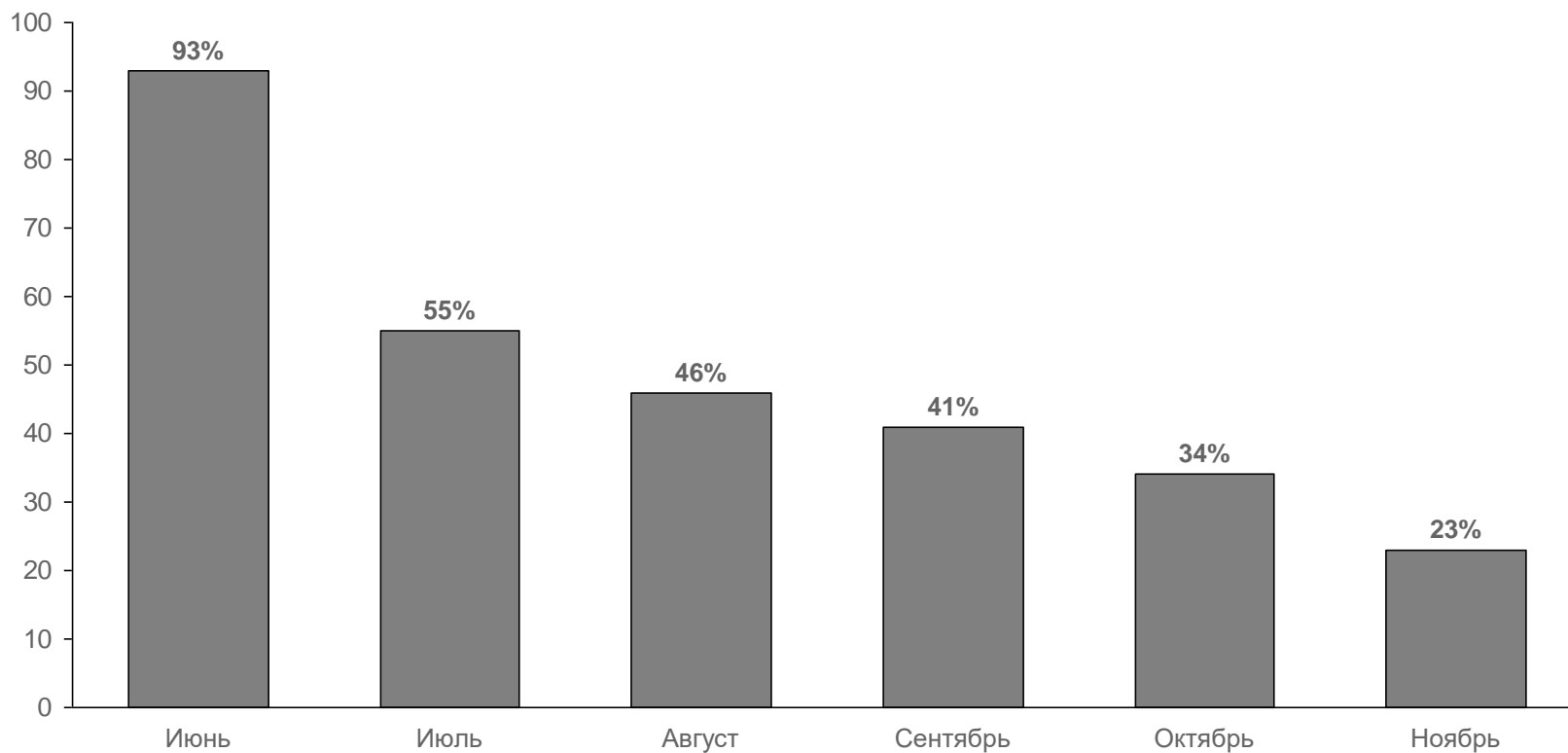
<sup>(1)</sup> 112 крупнейших по сборам проектов

Источник: анализ EY на основании данных Coindesk, Autonomous Next, Token Market, сайтов компаний

<sup>(2)</sup> Источник: State of European Tech Report 2017, Atomico

## Проектам становится все сложнее собирать цель: менее 25% в ноябре против 90% в июне

% проектов, собравших планируемую сумму





1. Статус рынка ICO
- 2. Применение открытого блокчейна и ICO**
3. Выбор платформы и смарт-контракт
4. Оценка токена
5. Безопасность
6. Регулирование
7. Что делать
8. Приложения

# Применение открытого блокчейна и ICO

- **Открытый** (open/ permissionless) **блокчейн** - медленная и дорогая база данных, которая обеспечивает гарантию консенсуса между независимыми участниками транзакции без привлечения централизованного посредника.
- **Основной успех проектов на открытых платформах блокчейн** приходится на сферу финансов и инфраструктуру для других блокчейн-проектов, а самый успешный кейс - это сам ICO на платформе Ethereum. Несмотря на множество прогнозов, практическое применение публичного блокчейна в других областях затруднено из-за низкой скорости и высокой стоимости транзакций при наличии эффективных централизованных решений.
- **Отсутствие обоснованной необходимости использования блокчейна и собственной валюты (токена)** - наиболее частая проблема White paper ICO проектов. В результате многие платформы остаются на стадии идеи, или их реализация отличается от заявленной. Проекты, которые доходят до промышленного запуска, начинают принимать для оплаты фиатные валюты, снижая ценность и стоимость токена.

## Большинство White paper умалчивают про необходимость блокчейна

Многие пытаются привлечь инвестиции через внедрение блокчейна в новых отраслях. White papers большинства проектов содержат много фраз-штампов, которые привлекают неискушенных инвесторов. Само обоснование необходимости блокчейна, как правило, отсутствует.

Хит-парад частых фраз White Papers :

- ...next generation platform
- ...first project to unlock multibillion market of <...>
- ...decentralized network that puts users in control \ driver's seat
- ...we are creating community \ ecosystem \ economy
- ...no corrupted central authority
- ...creating a Web3
- ...most undervalued token...
- ...making the world a better, blockchained place <sup>(1)</sup>
- ...the next decentralized worldwide cryptocurrency... to broaden the possibilities of uses and to increase the number of users by simplifying the process of managing cryptocurrency to the maximum <sup>(2)</sup>

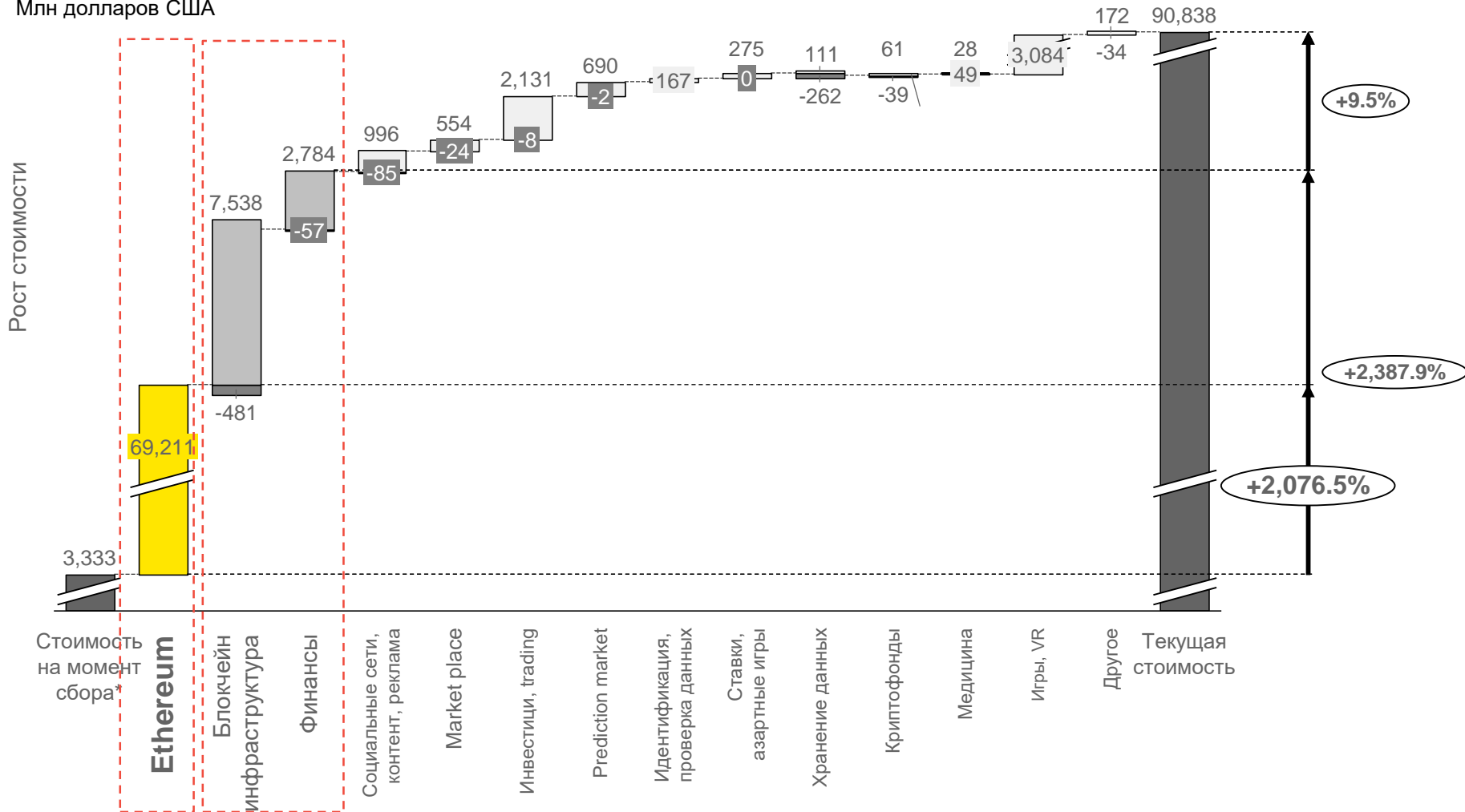
<sup>(1)</sup> "Silicon Valley"

<sup>(2)</sup> PlexCoin, активы заморожены ФБР  
Источники: сайты компаний

# Основной рост капитализации ICO проектов приходится на Ethereum и проекты блокчейн-инфраструктуры

## Рост капитализации проектов с момента сбора

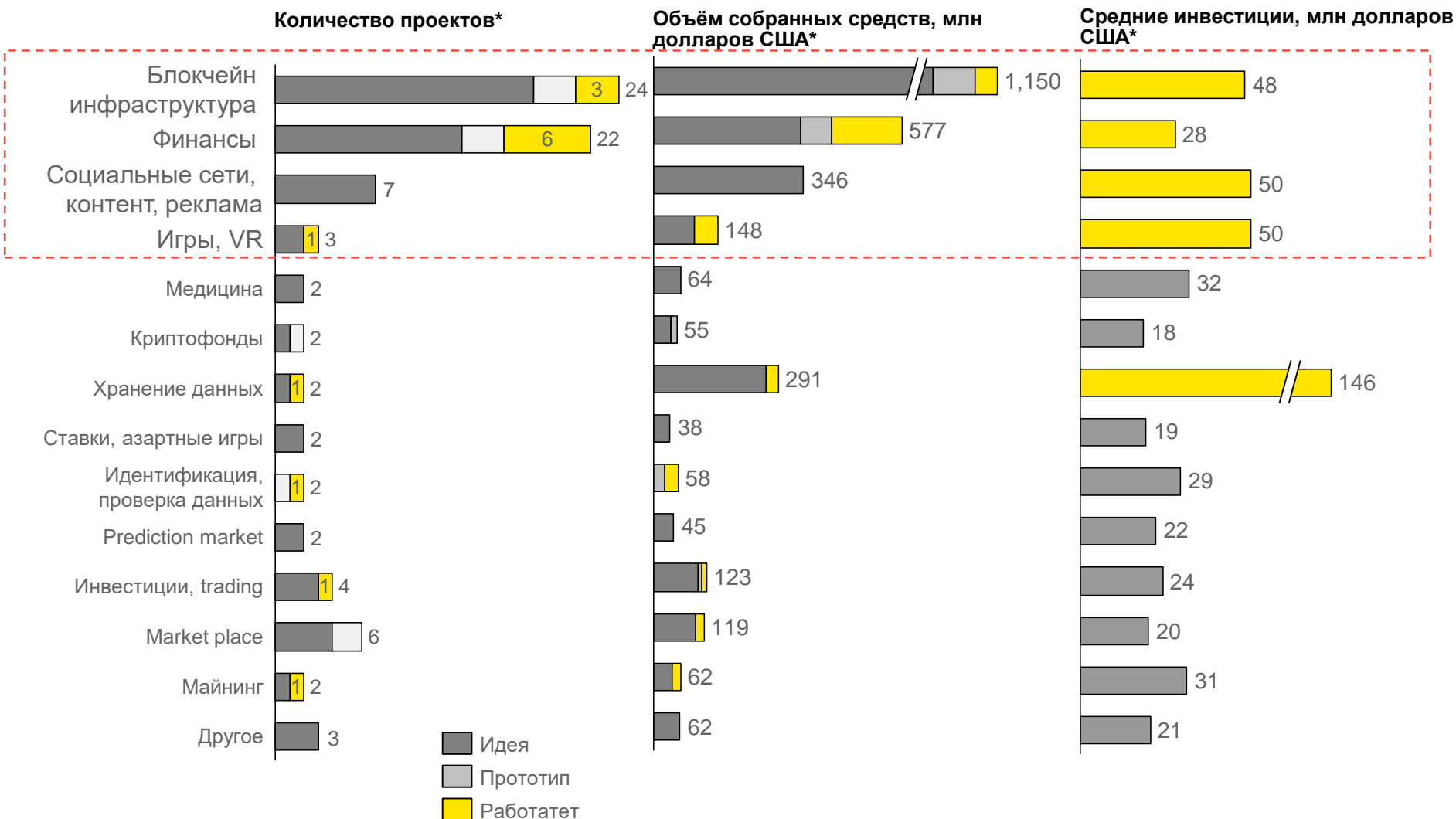
Млн долларов США



\* 111 проектов (87% всех сборов); текущая стоимость определена на 18.12.2017

Источник: анализ EY на основании данных Coindesk, Coinmarketcap, Autonomous Next, Token Market, сайтов компаний. В связи с большой волатильностью, данные на момент публикации и использования отчета могут существенно измениться.

# По объему инвестиций к лидерам роста добавляются игровые платформы, социальные сети и хранилища данных



# Технология полезна в ограниченном наборе случаев

**Открытый блокчейн - медленная и дорогая база данных, которая нужна для обеспечения гарантии консенсуса между независимыми участниками без централизованного посредника.** Отсутствие обоснованной необходимости использования блокчейн-функционала и собственной валюты (токена) - наиболее частая проблема ICO-проектов.

### Где открытый блокчейн хорошо

- Длинная цепочка субъектов, участвующих в транзакции, требующая последовательной синхронизации (поставки);
- Субъекты независимы, нет доверия;
- Субъекты готовы платить за проверку каждой записи;
- Существующий централизованный посредник дороже, чем блокчейн, есть риск безопасности;
- Ошибки при записи случаются редко, не требуют вмешательства посредника;
- Участники не против полной прозрачности транзакций;
- Никто из субъектов не контролирует более 50% узлов (для нового блокчейна);
- Есть четкие условия и гарантированные внешние источники информации (oracles) для смарт-контрактов;
- «Токенизация» активов.

### ...где не очень

- Необходима скорость транзакций;
- Мало узлов, и нет возможности обеспечить независимость консенсуса;
- Требуется анонимность / конфиденциальность транзакций;
- Надо обеспечить «право быть забытым»;
- Сложное ценообразование и риск манипуляций курса Utility token;
- Возможные изменения условий контрактов;
- Есть риск частых / существенных споров;
- Волатильность курса токена приводит к росту стоимости и потери конкурентоспособности услуг;
- Нет права на ошибку - случаются ошибки в реквизитах или суммах.

## Открытый блокчейн успешен в ограниченном наборе областей, собственный токен, как правило, не нужен

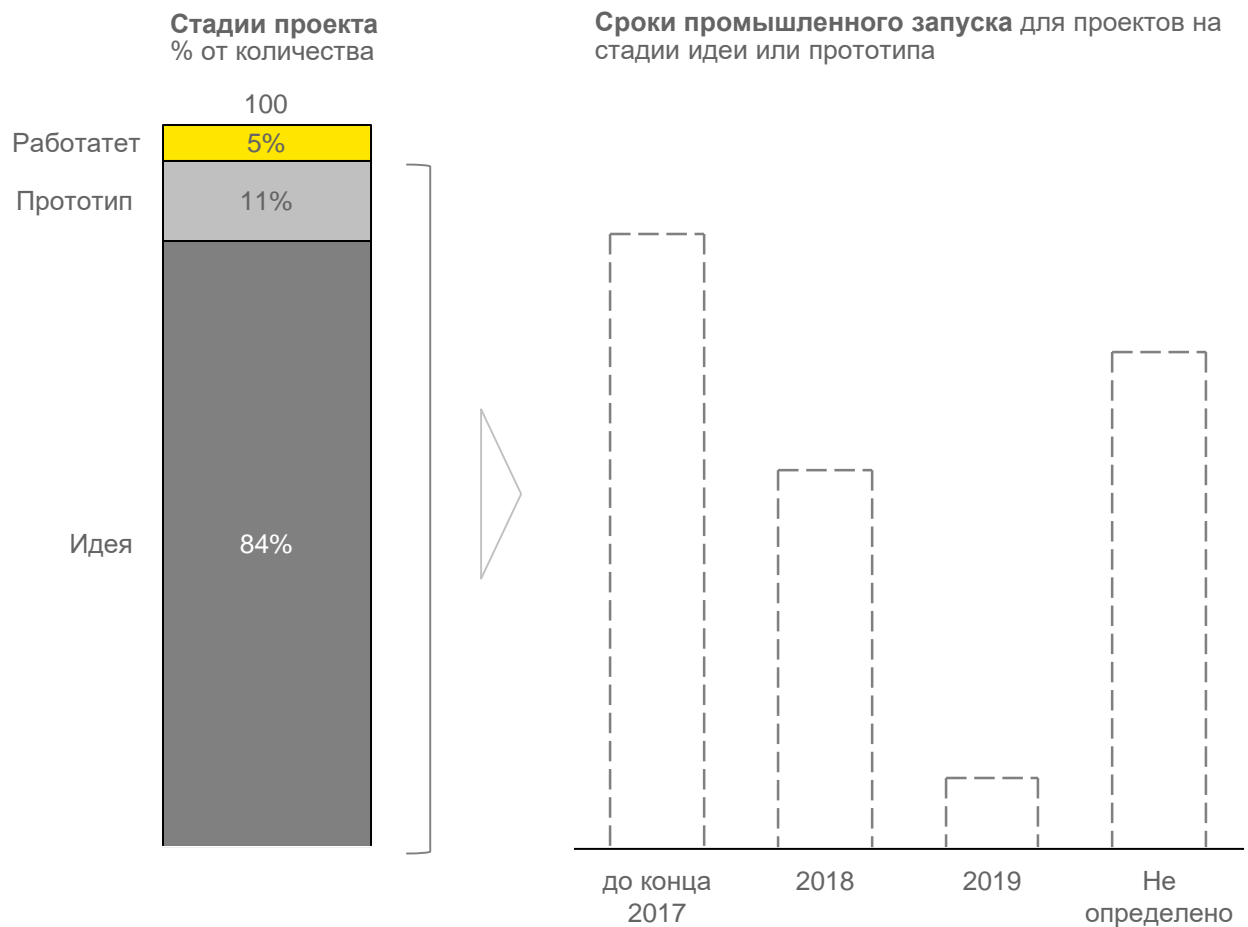
Несмотря на множество прогнозов, практическое применение публичного блокчейна в областях, отличных от финансов или инфраструктуры для других блокчейн-проектов, затруднено из-за низкой скорости, стоимости транзакций и неэффективного использования вычислительных ресурсов.

| Области                                    | Успешные кейсы блокчейн |          | Нужен свой токен? |
|--|-------------------------|----------|-------------------|
|  | Открытый                | Закрытый |                   |
| ICO  | Успешно                 |          | Да                |
| Финансы                                    | Успешно                 | ?        | Нет               |
| ID и персональные данные                   | ?                       |          | Нет               |
| Право собственности                        | ?                       |          | Нет               |
| Право пользования активами (shared use)    | ?                       |          | Да/Нет            |
| Голосование                                |                         | ?        | Да/Нет            |
| Поставки                                   | Успешно                 |          | Нет               |
| Энергоснабжение и поставки                 |                         | ?        | Да/Нет            |
| Прогнозы ("Prediction Markets" = Gambling) | ?                       | ?        | Нет               |

?
 Есть проекты в разработке, работающих успешный кейсов пока нет

## Запуск большинства проектов планируется через 1-2 года после ICO

**Идею продавать легче чем работающий сервис:** большинство ICO проектов находятся на стадии прототипа или идеи, промышленный запуск ожидается через год и более после ICO.





1. Статус рынка ICO
2. Применение открытого блокчейна и ICO
- 3. Выбор платформы и смарт-контракт**
4. Оценка токена
5. Безопасность
6. Регулирование
7. Что делать
8. Приложения

# Выбор платформы и смарт-контракт

- **Для ICO используют либо готовую, либо собственную блокчейн-платформу.** Во втором случае надо создавать сеть, привлекать и оплачивать услуги майнеров для подтверждения транзакций (консенсуса).
- **Большинство используют готовые платформы:** Omni, Waves, Ethereum, лидирующая с большим отрывом. Из-за популярности сеть Ethereum перегружена, растущий спрос повышает стоимость валюты Ether и, как следствие, стоимость ICO.
- **Условия ICO и функционал токена формулируются в смарт-контракте, который несет риски для всех участников.** Смарт контракт - это программный код, который может содержать случайные ошибки или преднамеренные “закладки”. Если сеть перегружена, то исполнение происходит с задержкой, что может повлиять на результат. Наиболее известные потери из-за смарт контрактов - DAO (потеря 65 млн долларов США) и Parity (200 млн долларов США).

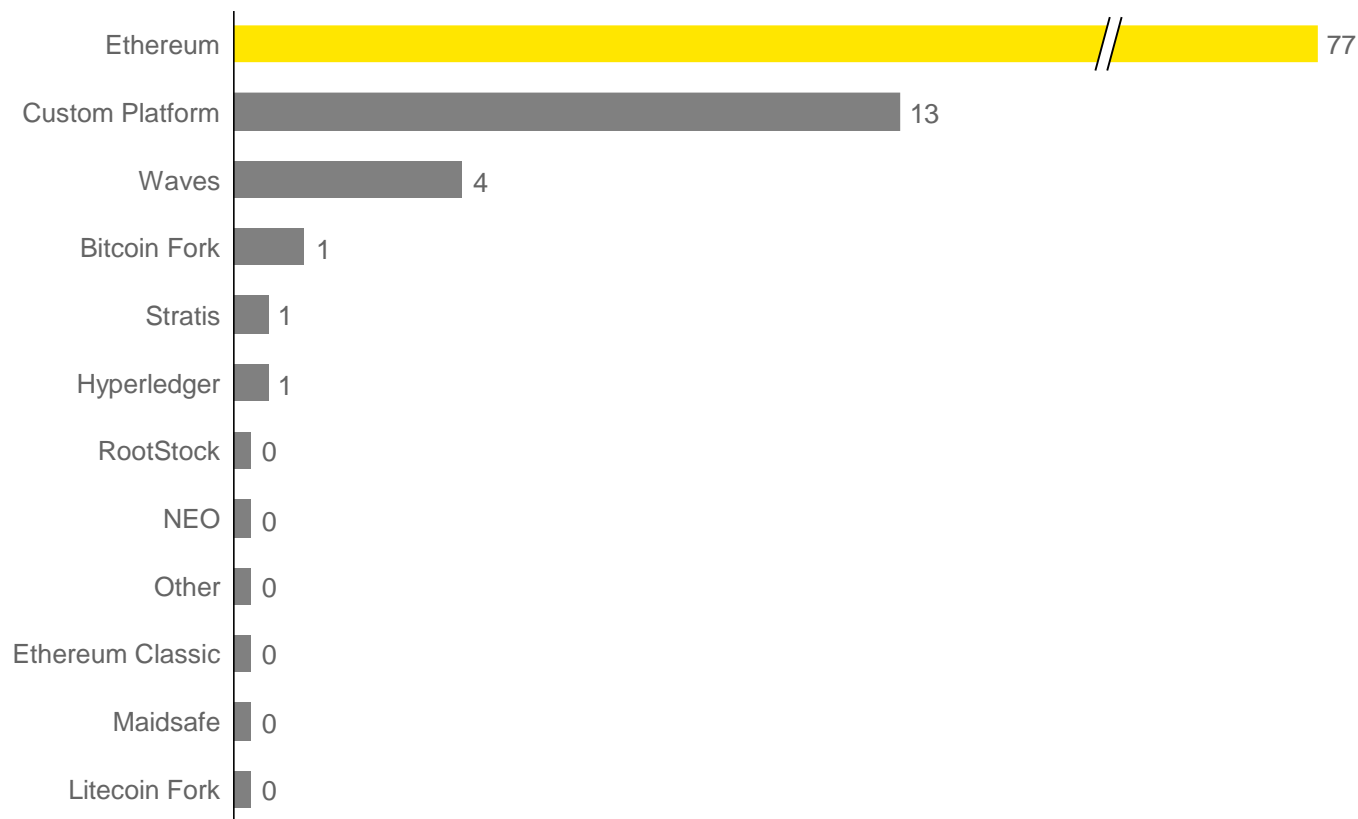
# Выбор платформы и смарт-контракт

## Ethereum - лидер ICO среди платформ

Для ICO используют либо готовую, либо собственную блокчейн-платформу. Во втором случае надо создавать сеть для подтверждения транзакций, привлекать и оплачивать услуги майнеров. Большинство используют готовые платформы: Waves, Omni, Bitcoin fork. Ethereum лидирует с большим отрывом.

### Распределение долей блокчейн-платформ при проведении ICO

% от всех проектов ICO



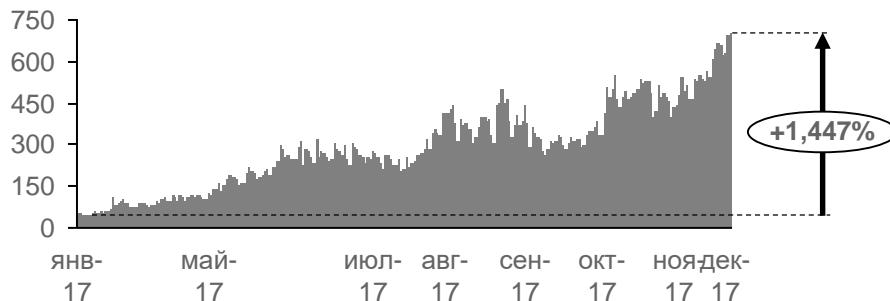
# Выбор платформы и смарт-контракт

## Ethereum: скорость падает, стоимость растет

Из-за популярности сеть Ethereum перегружена, растущий спрос повышает стоимость валюты Ether и, как следствие, стоимость ICO.

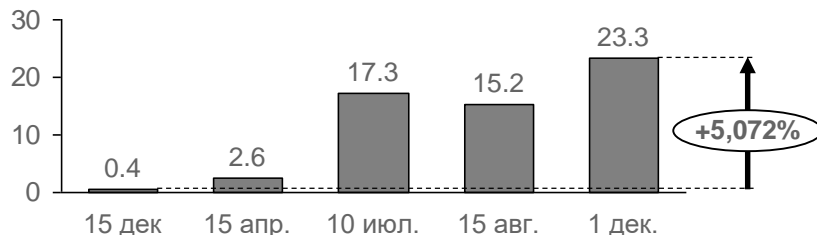
### Количество транзакций в сети Ethereum

Тысяч транзакций



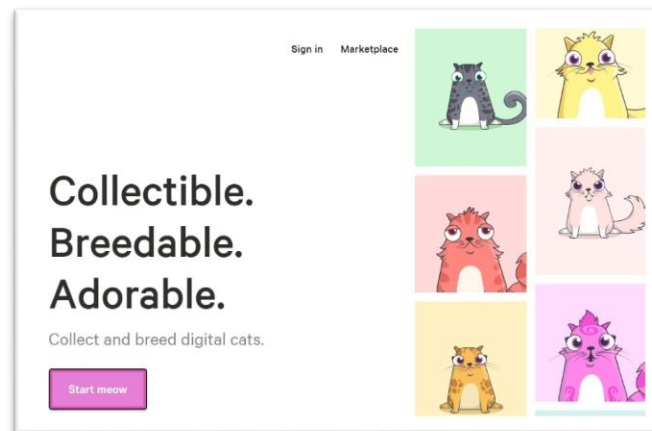
### Стоимости транзакции по развёртыванию условного смарт-контракта

долларов США



\*Данные для расчета: количество требуемого газа - 2 500 000 единиц. Цена газа в рассматриваемом периоде находилась на уровне 21-23 Gwei за единицу газа, цена Ether на определённую дату

28 ноября 2017 года Ethereum «поразил» феномен Cryptokittens: распределенное приложение по разведению виртуальных кошек, по аналогии с Тамагочи 90-х годов.



- Уже через неделю после выхода приложение отнимало до 21% от всей мощности сети.
- Из-за перегрузки многие компании отложили ICO. Некоторые планируют переход с Ethereum на другие платформы (например, Kik)
- Популярность Cryptokittens может привести к развитию аналогов, что еще больше прогрузит сеть и повысит стоимость расчета смарт контрактов.

# Смарт-контракт может содержать случайные уязвимости или преднамеренные закладки

Условия ICO и функционал токена формулируются в смарт-контракте. Это программный код, который может содержать случайные ошибки или преднамеренные “закладки”. Если сеть перегружена, то исполнение происходит с задержкой. Самые крупные потери из-за контрактов - DAO (65 млн долларов США) и Parity (200 млн долларов США) <sup>(1)</sup>.

### Наличие скрытых условий

Код смарт-контракта, реализующего условия ICO и функционал токена, может содержать скрытые условия которые в явном виде не раскрыты для инвесторов (пример: **Bancor**).

### Использование небезопасных алгоритмов

Недостаточное тестирование функционала смарт-контракта, а также использование внешних публичных библиотек, функционал которых может быть использован при реализации смарт-контракта, может повлечь за собой следующие последствия:

- Непреднамеренное нарушение логики функционала смарт-контракта и выполнение смарт-контракта с нарушением порядка и количества использованных функций, а также выполнение смарт-контракта с использованием нештатных функций (пример: **Parity**.)
- Преднамеренное внешнее воздействие на логику функционала смарт-контракта с целью обхода ограничений или для вывода средств (пример: **DAO**).

## Смарт-контракт: код может содержать скрытые условия

Код смарт-контракта, реализующего условия ICO одного из проектов, содержал условия, которые в явном виде не были раскрыты инвесторам. В результате стоимость токенов была «размыта».

### Что показывают инвесторам

Источник: Medium, сайт проекта

#### Terms Summary:

- **50/20/20/10 Token Distribution:** 50% of BNT will be issued to the contributors in the fundraiser, 20% allocated to partnerships, community grants and public bounties, 20% to the Foundation's long-term operating budget, 10% to founders, team members, advisors and early contributors. Founders and team contributors will be subject to a three year vesting schedule.
- **Fixed Price:** 0.01 ETH per 1 BNT (i.e. 100 BNT per 1 ETH)
- **Hidden ETH Cap:** revealed if 80% of the cap is reached.
- **Duration:** The fundraiser will run for 14 days or until the hidden cap is reached, with a 1 hour minimum time.
- **How minimum time works?** Read this: <https://goo.gl/1L0NY>
- **Token Availability:** BNT for ETH contributions will be distributed immediately. The ability to transfer, purchase and liquidate BNT through the smart token's contract will be enabled gradually during a time span estimated at 7 days following the fundraiser closing.
- **Security:** Funds will be held using multi-sig wallets according to industry best practices.

### Что исполняется

Источник: Etherscan

#### Contract Source Code </>

```
456 {
457     return processContribution();
458 }
459
460 /**
461  * @dev handles contribution logic
462  * note that the Contribution event is triggered using the se
463  *
464  * @return tokens issued in return
465  */
466 function processContribution() private
467     active
468     etherCapNotReached(msg.value)
469     validGasPrice
470     returns (uint256 amount)
471 {
472     uint256 tokenAmount = computeReturn(msg.value);
473     assert(beneficiary.send(msg.value)); // transfer the ether
474     totalEtherContributed = safeAdd(totalEtherContributed, msg
475     token.issue(msg.sender, tokenAmount); // issue new funds t
476     token.issue(beneficiary, tokenAmount); // issue tokens to
477
478     Contribution(msg.sender, msg.value, tokenAmount);
479     return tokenAmount;
```

### Текст для инвесторов, 18 строк

During the first hour, all funds would be allowed in. If the sale goes over the “hidden cap”, it would stop immediately at the end of this first hour”

В тексте описания нет:

### Функционал заложенный в коде, 479 строк

Команда проекта может изменять срок проведения ICO когда и на сколько угодно, размывая стоимость токенов.

Команда может блокировать все транзакции с использованием токена в любое время и по любой причине.

Команда может выпускать новые токены в любое время.

Команда может уничтожить токены с любого счёта в любое время.

1. Статус рынка ICO
2. Применение открытого блокчейна и ICO
3. Выбор платформы и смарт-контракт
4. **Оценка токена**
5. Безопасность
6. Регулирование
7. Что делать
8. Приложения

# Оценка токенов

- **Оценка токена больше похожа на оценку золота или модной вещи в высокий сезон, когда ограниченное предложение не способно удовлетворить ажиотажный спрос.** При сбалансированном спросе она должна определяться традиционными методами - прогнозами развития проекта и природой токена. Но в большинстве случаев она определяется PR, качеством White paper и техникой ICO-продаж.
- **Традиционная оценка токена как валюты зависит от параметров, которые на стадии разработки определить сложно.** Она определяется балансом между количеством токенов ( $T$ ) и их оборачиваемостью за период ( $V$ ) со стоимостью ( $P$ ) и объемом услуг ( $Q$ ) на платформе за тот же период:  $TV = PQ$ . Другие типы токенов (ценная бумага или актив) практически не используются.
- **Кроме того, токен имеет двойную природу, что еще больше затрудняет оценку.** Инвесторы ожидают роста цены токена, клиенты платформы - падения стоимости услуги, которая выражается в токенах. Т.е. стоимость токена обратно пропорциональна стоимости единицы услуг.
- **Поэтому подготовка и техника проведения ICO – основное, что определяет капитализацию и стоимость токена.** Два основных способа: 1) объем привлечений ограничен, и токены реализуются по фиксированной цене (Capped), 2) объем не ограничен, токены распределяются после окончания ICO пропорционально всем инвестициям (Uncapped). Первый способ, как правило, создает ажиотаж и распродажу всем, кто успел. Во втором случае доля токенов, которые получает инвестор, сильно размывается из-за большого объема и неопределенности стоимости до закрытия ICO. Многие инвесторы стараются ждать до последнего, создавая шквал заявок перед закрытием, что перегружает сеть.



# Оценка должна определяться прогнозами развития проекта и природой токена. Но по факту определяется ажиотажем

Большинство проектов - это платформа / marketplace. Наиболее частый тип токена – средство оплаты (валюта) услуг на этой платформе. Оценка валюты зависит от множества переменных и крайне сложна для проектов на стадии разработки. Поэтому оценка определяется проведением PR, качеством White paper и организацией торгов.

## Как должен оцениваться токен:

Типы токена и прогнозы

|   |   |
|---|---|
| Ценная бумага   | DCF, Мультипликаторы  |
| Актив   | Определяется стоимостью актива, который обеспечивает токен  |
| Средство оплаты на платформе (utility token - частная валюта) | Определяется балансом между количеством токенов (T) и их оборачиваемостью (V) со стоимостью услуг (P) и объемом их продаж за период: $TV = PQ$            |
|   | Динамика стоимости товара в токенах обратна пропорциональна динамике стоимости токена, что сильно усложняет оценку и ценообразование, ограничивает рынок. |
|   | Поэтому при запуске платформы часто дают возможность оплаты в фиатных валютах, что обесценивает токен   |

## Как оценивается на самом деле:

Раскрутка и техника ICO торгов

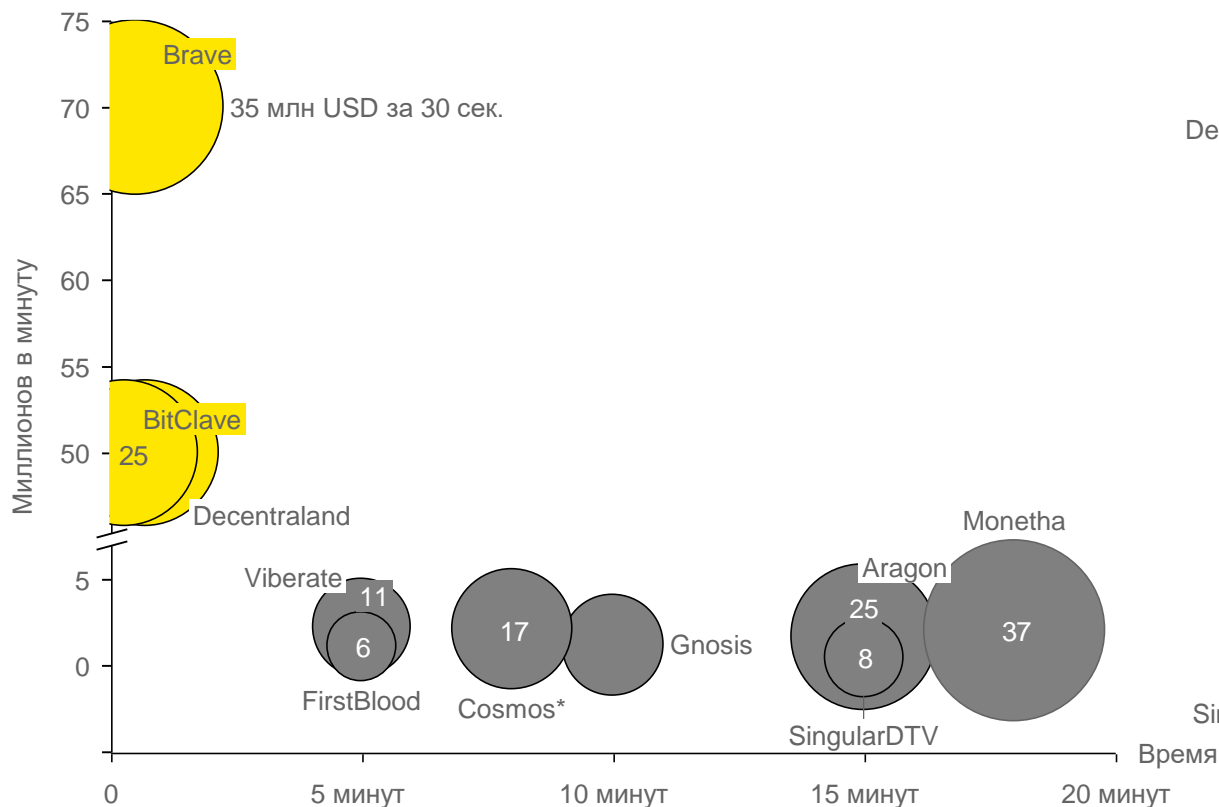
|  |  |
|--|--|
| Ограничения по времени \ объему инвестиций | <b>CAPPED:</b> ограниченное количество токенов по фиксированной цене. Как правило создает ажиотаж (FOMO*) и распродажу за секунды.   |
| Валюта инвестиций                          | <b>UNCAPPED:</b> распределение токенов пропорционально инвестициям. Из-за неопределенности стоимости токена до закрытия ICO, инвесторы стараются ждать до последнего, шквал заявок перед закрытием перегружает сеть. |
| Баунти (дисконт для ранних инвесторов)     | Продажа токенов в нескольких валютах на нескольких платформах. Возможность арбитража на разнице курсов   |
| Возможность выпуска \ изъятия токенов      | Баунти-токены часто распродают после начала торгов, что обрушает стоимость токена.   |
|  | Увеличивает неопределенность стоимости токена и волатильность при начале торгов  |

# Опасения «не успеть» заставляют инвесторов перечислять средства с рекордной скоростью

**Capped\*** продажи раскрученных проектов создают беспрецедентный ажиотаж, время проведения отдельных ICO сокращается до минут. 10 проектов рекордсменов привлекали средства со средней скоростью 300 тыс. долларов США в секунду. Brave (BAT) - 1166 тыс. долларов США в секунду

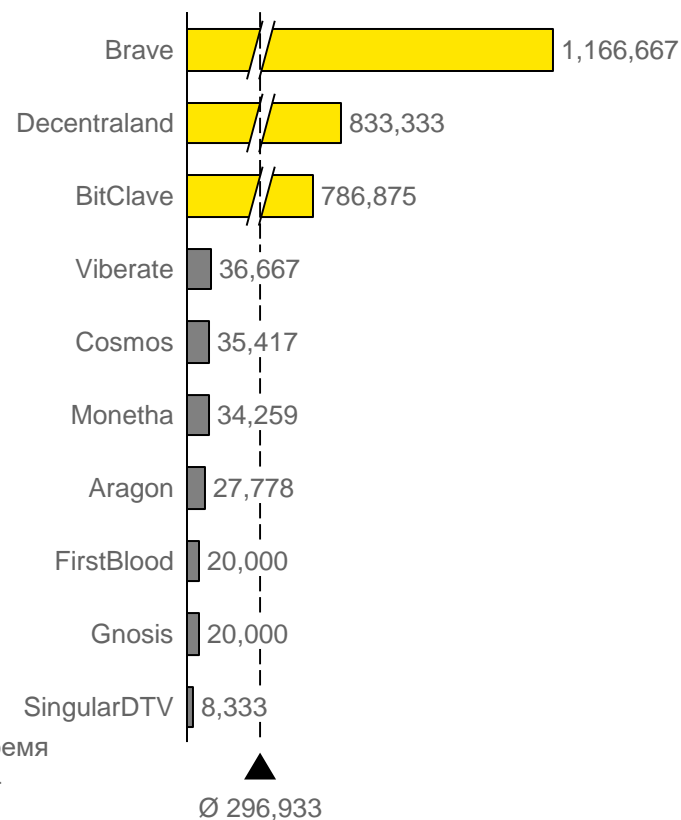
## Объем и скорость сбора средств

Млн долларов США в минуту



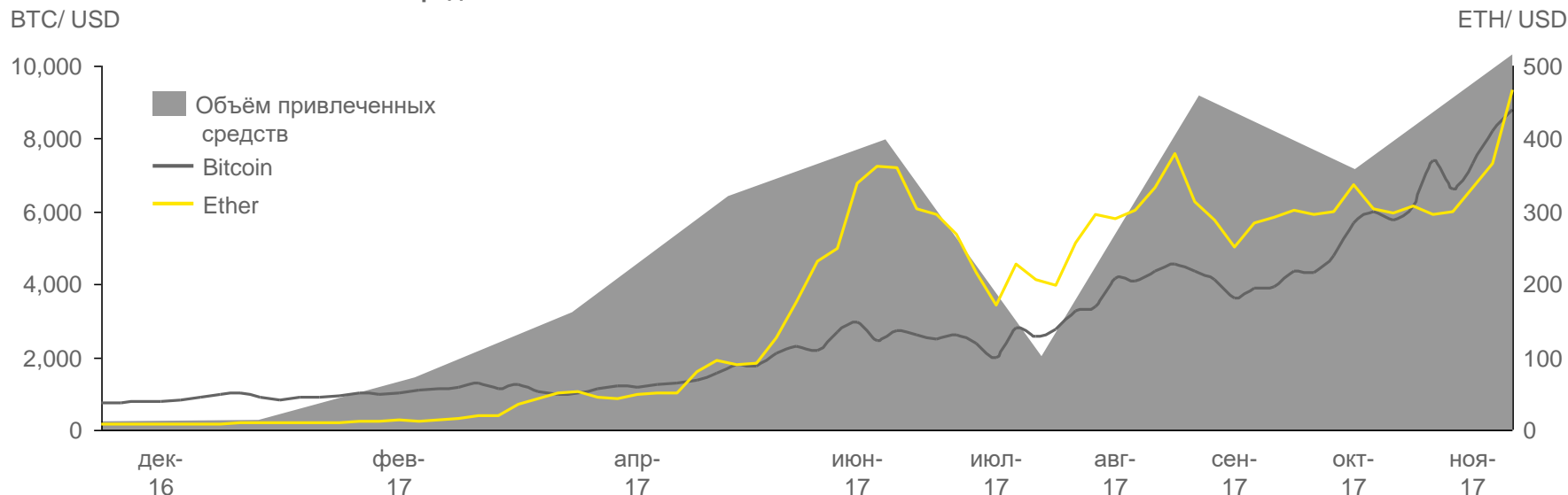
## Скорость сбора

долларов США в секунду

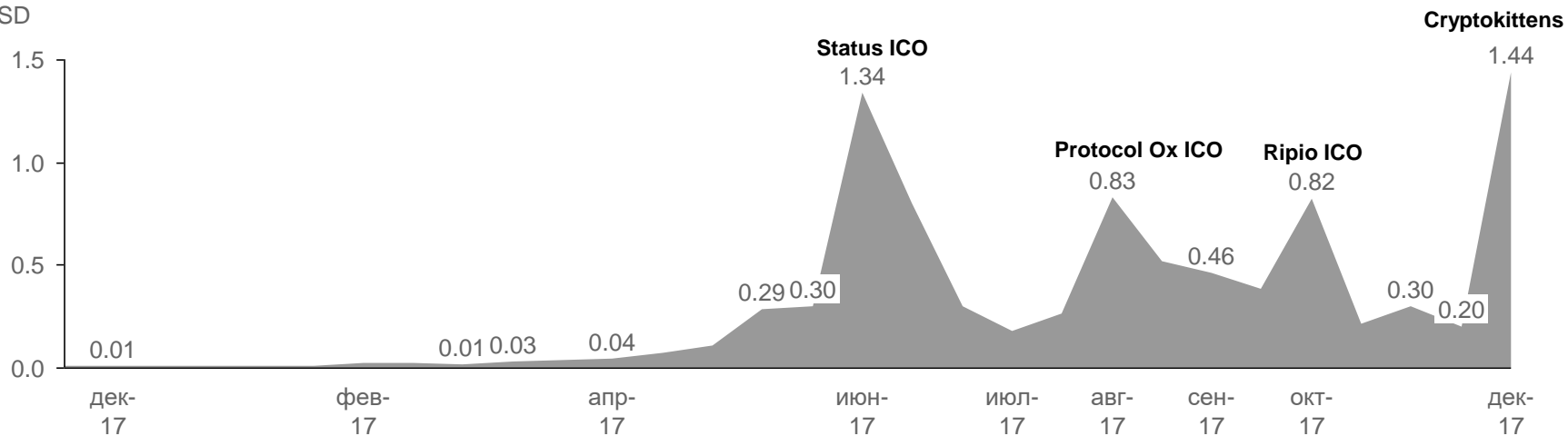


# ICO увеличивает спрос на Ether и BTC: рост курса Ether ведёт к увеличению стоимости транзакций в сети Ethereum

Рост стоимости BTC ETH / объём средств ICO  
BTC/ USD



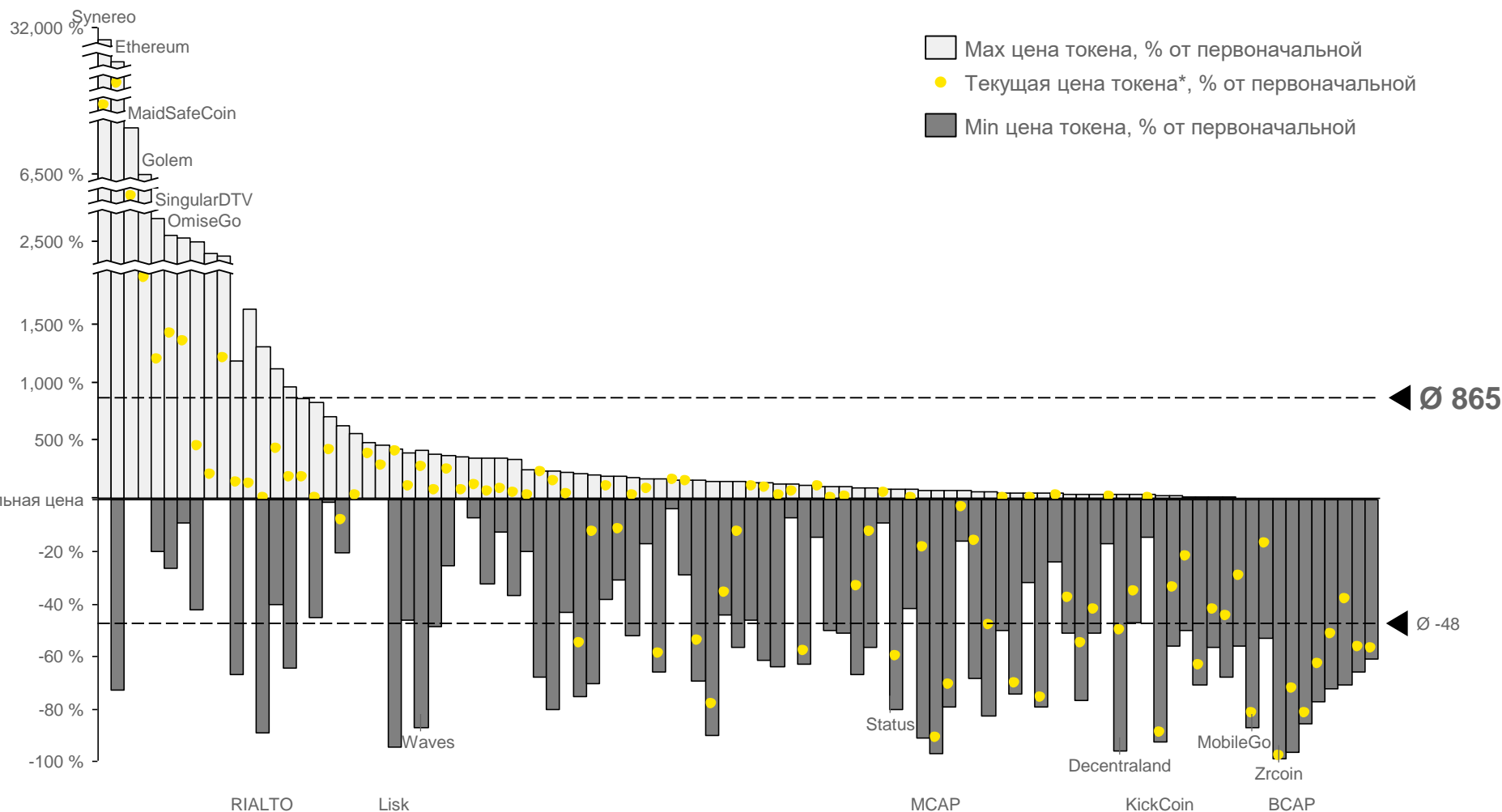
Средняя стоимость транзакции в сети Ethereum, USD



# Оценка токенов

## Отсутствие возможности фундаментальной оценки приводит к экстремальной волатильности после начала торгов токеном

Изменение цены токена  
% от первоначальной



\*Начальная цена: первая цена при листинге на бирже. Текущая цена: на 16.11.2017

Источник: на основании данных с Coinmarketcap

В связи с большой волатильностью, данные на момент публикации и использования отчета могут существенно измениться.

1. Статус рынка ICO
2. Применение открытого блокчейна и ICO
3. Выбор платформы и смарт-контракт
4. Оценка токена
- 5. Безопасность**
6. Регулирование
7. Что делать
8. Приложения

# Безопасность

- **Объемы ICO вызывают всплеск интереса хакеров.** В среднем более 10% средств от ICO теряются в результате атак. Хакерам помогают ажиотаж, отсутствие централизованного арбитра и необратимость транзакций на БЧ.
- **Основатели фокусируются на привлечении инвесторов, безопасность часто уходит на второй план.** Хакеры успешно этим пользуются. Чем более «раскрученный» и масштабный ICO, тем более он привлекателен для атак.
- **Атакам подвергаются как проекты (эмитенты) так и инвесторы.** Основные инструменты отъема средств: подмена адреса кошелька проекта, получение доступа к закрытым ключам и кража средств с кошельков, взломы бирж и кошельков.
- **На долю фишинговых схем приходится более половины всех хищений.** В начале весны 2017 года этот тренд начал стремительно расти. Это можно объяснить простотой и чрезвычайной результативностью таких атак.
- **Кроме потери средств взломы приводят к косвенным потерям.** Для проекта – это потеря репутации. Для инвесторов – это потеря персональных данных, которые необходимы для процедуры KYC\* или для торговли на крипто-биржах.

# Участники ICO сразу становятся мишенью для атак

**Объемы ICO вызывают всплеск интереса хакеров.** В среднем более 10% средств от ICO теряются в результате атак. Хакерам помогают ажиотаж, отсутствие централизованного арбитра и необратимость транзакций в блокчейн. Основные виды атак:

- Фишинговые сайты
- DDoS атаки
- Взлом сайта / веб-приложения
- Атаки через сотрудников компании
- Атаки на IT-инфраструктуру проектов
- Атаки на инвесторов

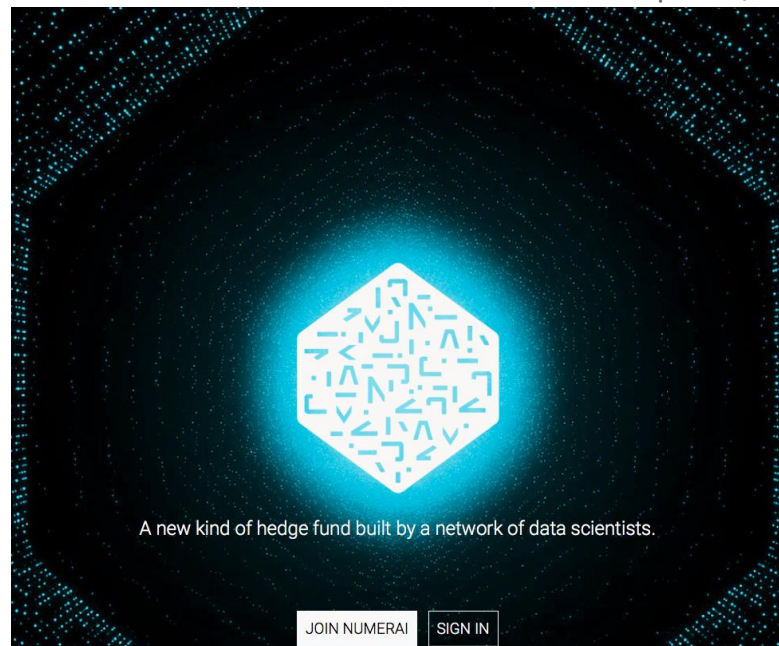
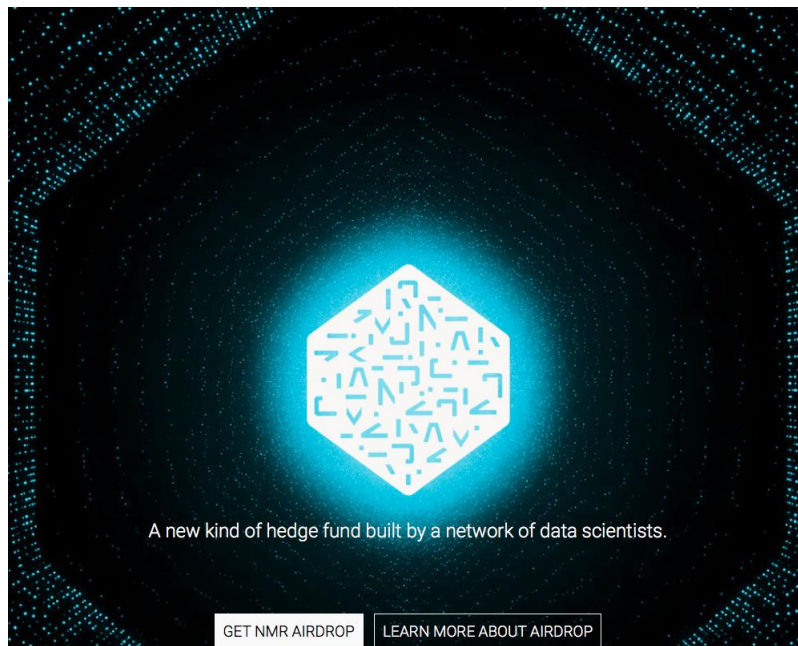
## На долю «фишинга» приходится более половины всех хищений

**Фишинговые сайты - клоны официального ресурса, самый распространенный вариант хищения средств.** Его популярность можно объяснить простотой и результативностью таких атак: доход хакеров может достигать до **1,5 млн** долларов США в месяц. Как правило, через фишинговый сайт мошенники либо предлагают перевести средства на свой кошелек или контракт, либо выманивают приватный ключ от кошелька инвестора.

Оригинал

Пример: хедж-фонд Numeraire (США)

Фишинговая страница



Клон зарегистрирован 9 августа 2017г. и распространялся через мессенджер Slack от имени «сотрудника» хедж-фонда. Злоумышленники выманивали приватный ключ и выводили все средства с аккаунта пользователя. Эти же мошенники создали копии сайтов 7 других криптовалютных проектов. Только в августе 2017 они аналогичным образом опустошили почти 350 кошельков на **1,4 млн долларов США**.

«Фишеры» настраивают контекстную рекламу в поисковиках и забрасывают адреса фишинговых сайтов во все каналы коммуникации. Легитимные пользователи в ажиотаже ICO зачастую не проверяют сайт, на котором покупают токены.



# Взломы бирж приводят как к потере средств, так и к потере персональных данных

Две группы рисков хранения и торговли токенами после ICO: потеря средств и потеря персональных данных

### Потери средств

Средняя потеря при взломе криптобиржи – 2 млрд долларов США\*. Для сравнения: средняя потеря банка – до 1,5 млн долларов США, при этом средства, как правило, застрахованы.

Криптовалютные биржи привлекают большее внимание, чем банки: анонимность, необратимость транзакций, а также ажиотаж и информационный хаос. Если пользователи лишаются своих средств, вероятность возврата украденных монет близка к нулю.

### Потеря персональных данных

Для совершения операций большинство крупных бирж требуют расширенную идентификацию:

- Фотокопии документов удостоверяющих личность
- Фотокопии кредитных карт
- Действующий телефон
- Реквизиты банковских счетов.

Как правило, биржи не раскрывают наличие контролей над хранением и использованием персональных данных, которые представляют большую ценность на черном рынке. В случае взлома биржи вероятность неправомерного использования такой информации крайне велика.

## Взломы бирж происходят регулярно, частота атак растет

Подверглась хакерской атаке через уязвимость хостинг-площадки сервиса. Средства выведены, биржа закрылась

**Bitcoinica**

Bitcoinica  
43 000 BTC



Хакер смог получить доступ к резервному хранилищу ключей от кошелька биржи. Биржа закрылась, часть средств возвращена пользователям

**bitfloor**

Bitfloor  
25 000 BTC



Биржа закрыла сайт и объявила о взломе. Позднее биржа подала на банкротство. Пользователи не получили компенсации. Попытки взлома были в 2012 году.

**MT.GOX**

Mt Gox  
850 000 BTC



Фишинг. В результате реорганизация всей трейдинговой платформы. Потери покрыты из резервных средств.

**BITSTAMP**  
SECURE TRADING AND MONEY PAYMENT

Bitstamp  
19 000 BTC



**BITFINEX**

Bitfinex  
119.456



Биржа не использовала «холодное хранение». Работы были восстановлены. Биржа выпустила токены Bitfinex (BFX) для пользователей, которые потеряли свои средства. Потерянные средства возмещены полностью.

**bithumb**

Bithumb  
420 BTC



Злоумышленники сумели скомпрометировать компьютер одного из сотрудников. Работа восстановилась, были выплачены частичные компенсации.

Объем украденных с биржи средств в биткоинах

Март  
2012

Сентябрь  
2012

Февраль  
2014

Январь  
2016

Август  
2016

Июль  
2017

1. Статус рынка ICO
2. Применение открытого блокчейна и ICO
3. Выбор платформы и смарт-контракт
4. Оценка токена
5. Безопасность
- 6. Регулирование**
7. Что делать
8. Приложения

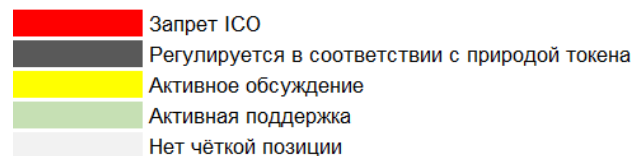
# Регулирование

- **Большинство стран двигаются по схожей траектории - от игнорирования ICO до его запрета либо регулирования токена в соответствии с его природой.** Но трактование природы токенов может сильно различаться между странами: иное имущество, акции, право требования, валюта.
- **Отраслевые ассоциации вырабатывают собственные принципы, чтобы заполнить регуляторный вакуум.** Один из наиболее интересных - SAFT (Safe Agreement for Future Token), в соответствии с которым инвесторы получают опцион, который действует до момента запуска платформы, когда токен можно использовать как средство платежа.
- **Регуляторы начинают активно вовлекаться при признаках нарушения законодательства:** о валютном контроле, о рынке ценных бумаг, ПОД/ФТ\*, налогового, уголовного, о персональных данных. Комиссия по ценным бумагам США создала специальное подразделение и завела минимум два дела по подозрению в мошенничестве при реализации проектов ICO.
- **В РФ пока нет единой позиции в отношении криптовалют.** Общий настрой: блокчейн хорошо, биткоин нет, ICO надо регулировать как IPO. Но в соответствии с действующим законодательством рубль — это пока единственный инструмент расчета, а создание валютных суррогатов запрещено.

# Регулирование Основной риск – неопределенность

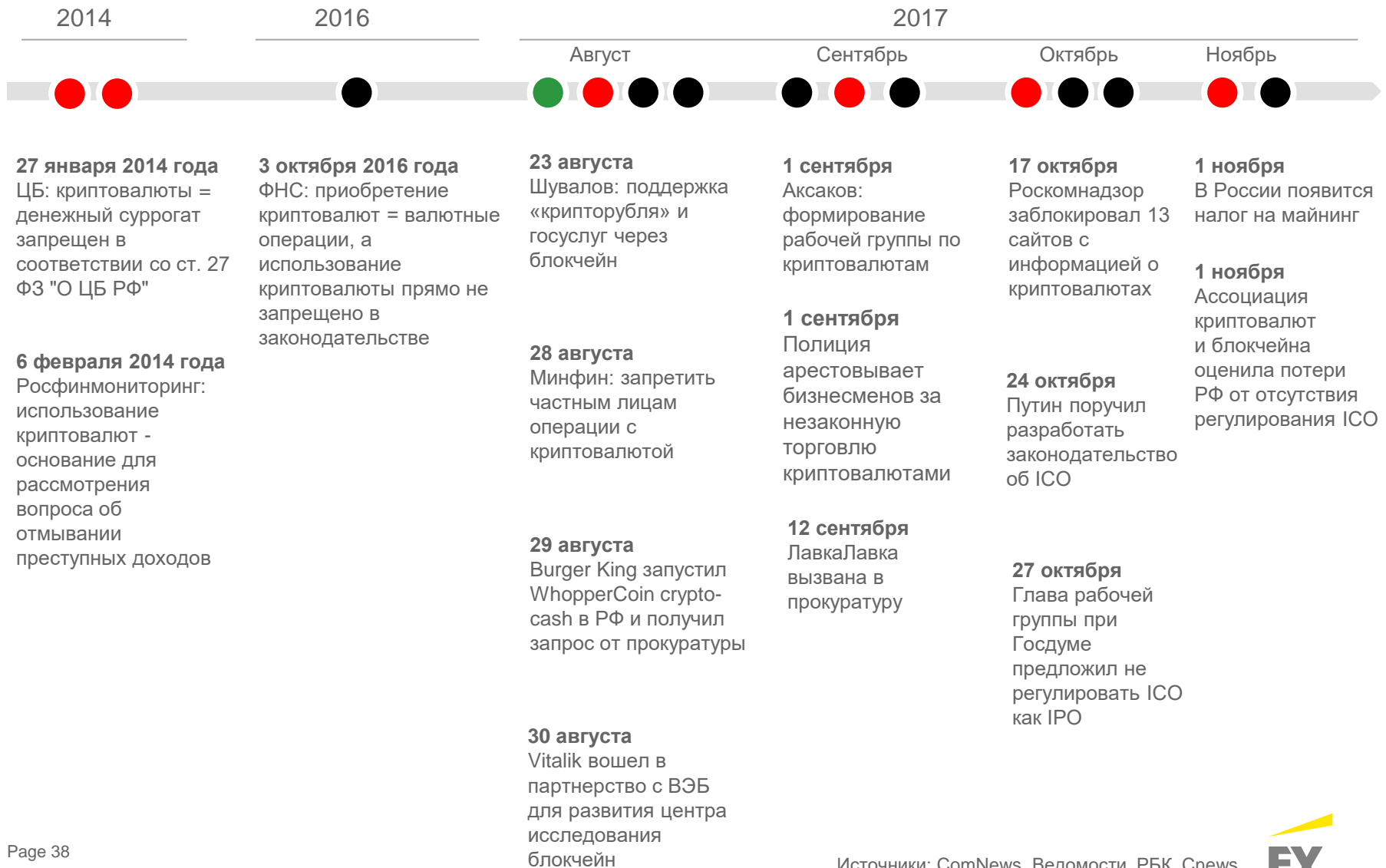
«Не знаешь, откуда прилетит»: ICO привлекает инвестиции и планирует деятельность далеко за рамками одной страны. Большинство стран движутся от игнорирования ICO до его запрета, либо регулирования токена в соответствии с его природой. Но трактование природы токенов может сильно различаться между странами.

|                | 2008-2015 | 2016                | 2017  |   |   |
|----------------|-----------|---------------------|---|---|---|
|                |           |                     | Январь - Июнь                                 | Июль - Сентябрь                               | Сентябрь - Ноябрь                             |
| Китай          |           | Активное обсуждение | Активное обсуждение                           | Запрет ICO                                    | Запрет ICO                                    |
| США            |           |                     | Активное обсуждение                           | Регулируется в соответствии с природой токена | Регулируется в соответствии с природой токена |
| Великобритания |           |                     | Активное обсуждение                           | Активное обсуждение                           | Активное обсуждение                           |
| Канада         |           |                     |   | Регулируется в соответствии с природой токена | Регулируется в соответствии с природой токена |
| Сингапур       |           | Активная поддержка  | Активная поддержка                            | Активная поддержка                            | Регулируется в соответствии с природой токена |
| Гонконг        |           |                     |   | Активное обсуждение                           | Регулируется в соответствии с природой токена |
| Австралия      |           |                     |   | Активное обсуждение                           | Регулируется в соответствии с природой токена |
| Швейцария      |           | Активная поддержка  | Активная поддержка                            | Активная поддержка                            | Активное обсуждение                           |
| Япония         |           | Активное обсуждение | Регулируется в соответствии с природой токена | Регулируется в соответствии с природой токена | Регулируется в соответствии с природой токена |
| Остров Мэн     |           | Активная поддержка  | Активная поддержка                            | Активная поддержка                            | Активная поддержка                            |
| Малайзия       |           | Активное обсуждение | Активное обсуждение                           | Активное обсуждение                           | Активное обсуждение                           |
| Эстония        |           |                     |   | Активная поддержка                            | Регулируется в соответствии с природой токена |
| Южная Корея    |           |                     |   | Активное обсуждение                           | Запрет ICO                                    |
| <b>Россия</b>  |           | Активное обсуждение | Активная поддержка                            | Активное обсуждение                           | Активное обсуждение                           |
| Новая Зеландия |           |                     |   |   | Регулируется в соответствии с природой токена |
| Литва          |           |                     |   |   | Регулируется в соответствии с природой токена |



# Регулирование В РФ нет единой позиции в отношении криптовалют

Предложения по регулированию разнонаправлены. Общий настрой: блокчейн хорошо, биткоин нет, ICO надо регулировать как IPO. Но в соответствии с действующим законодательством рубль — это пока единственный инструмент расчета, а создание валютных суррогатов запрещено.



# В условиях неопределенности участники рынка самостоятельно пытаются повысить прозрачность ICO

Май 2017

Август 2017

Сентябрь 2017

Октябрь – Декабрь 2017

## Simple Agreement for Future Tokens (SAFT)

Разработанный Protocol Labs инвестиционный контракт между организатором ICO и аккредитованным инвестором, предоставляющий опционы на покупку токенов, совместимый с правовыми нормами США. Опцион действует до запуска платформы, после чего обменивается на utility-токены

## Российская ассоциация криптовалют и блокчейна (РАКИБ)

Ассоциация разработчиков и пользователей технологии блокчейн и продуктов, созданных на ее основе. Содействует распространению и интеграции блокчейна в экономику страны. Координация предпринимательской деятельности членов Ассоциации, представительство и защита их имущественных интересов.

## ICO Code of Conduct

Инициатива Crypto Valley Association (Швейцария) по разработке официального Кодекса проведения ICO, который поможет избежать рисков и неправомерного поведения со стороны организаторов ICO.

## ICO Governance Foundation

Международная организация, целью которой является защита инвесторов ICO и содействие формированию капитала для ICO. IGF инициировала открытую добровольную форму регистрации ICO (Form IGF-1). Сотрудничает с национальными регуляторами с целью создания методов и стандартов для регулирования ICO, дополняющих существующее регулирование SEC, ESMA, CSRC, MAS.

## ICO Transparency Initiative

Инициатива 16-ти блокчейн-проектов, направленная на поощрение раскрытия данных о кошельках, контролируемых проектом, и объяснение любых расходов, превышающих 0,5% собранных средств.

## Token Alliance

Инициатива торговой ассоциации Chamber of Digital Commerce, направленная на разработку стандартов для ICO, а также для решения вопросов, связанных с регулированием SEC.

## Ассоциация по регулированию ICO (инициатива Waves)

Создание ассоциации, которая займётся разработкой стандартов отчетности, налогового и бухгалтерского учета, вопросами соблюдения принципов KYC и различными нормативно-правовыми аспектами для ICO и блокчейн-индустрии.

1. Статус рынка ICO
2. Применение открытого блокчейна и ICO
3. Выбор платформы и смарт-контракт
4. Оценка токена
5. Безопасность
6. Регулирование
7. **Что делать**
8. Приложения



# Что дальше

ICO для многих стал синонимом ажиотажа и неприемлемого риска, объемы привлечений начинают постепенно снижаться. С другой стороны, правильное применение блокчейн может обеспечить как защиту инвесторов, так и эффективное финансирование качественных проектов.

Исходя из накопленного опыта, в дополнение к стандартным шагам участникам ICO необходимо:

- |                    |   |
|--------------------|---|
| <b>Проектам</b>    | <ul style="list-style-type: none"><li>• Проработать понятное для инвесторов обоснование преимущества блокчейна и собственного токена в предлагаемом проекте.</li><li>• Использовать итерационный процесс ICO аналогично IPO, чтобы сделать понятным диапазон цен токена и обеспечить возможность участия всех заинтересованных инвесторов.</li><li>• Подготовить и зарегистрировать понятную инвесторам юридическую структуру.</li><li>• Обеспечить информационную безопасность средств и персональных данных, как во время ICO так и после.</li><li>• Обеспечить соответствие действующему законодательству не только в стране регистрации, но и во всех странах, где планируется деятельность и обращение токена.</li></ul>   |
| <b>Инвесторам</b>  | <ul style="list-style-type: none"><li>• Использовать прозрачность открытых блокчейн для анализа проекта: в дополнение к стандартной информации проводить анализ кода смарт-контракта, кода и статистики платформы.</li><li>• Инвестировать в те проекты, в которых кроме денег инвестор может привнести экспертизу («smart money»). Предложение проектов уже превышает спрос, инвесторам есть из чего выбрать.</li></ul>  |
| <b>Регуляторам</b> | <ul style="list-style-type: none"><li>• ICO - это новый механизм обычных хозяйственных отношений, который не должен выпадать из правового поля. Необходимо привязать терминологию «криптоэкономики» к существующим определениям, в ограниченных случаях ввести новые.</li><li>• Открытые блокчейн позволяют автоматизировать отчетность и повысить прозрачность проектов. Необходимо стандартизировать минимальные требования к такой отчетности.</li><li>• Защитить права держателей токена до появления возможности использовать его по назначению.</li><li>• Формализовать порядок оборота токенами, изменения их количества и функционала.</li><li>• Взаимодействовать с регуляторами других юрисдикций. Как минимум с теми, где проходит наибольшее количество ICO, базируются основные инвесторы и биржи.</li></ul> |

1. Статус рынка ICO
2. Применение открытых блокчейн и ICO
3. Выбор платформы и смарт контракт
4. Оценка токена
5. Безопасность
6. Регулирование
7. Что делать
8. Приложения

# Термины и определения

Терминология блокчейн и ICO пока формируется, единых утвержденных понятий пока нет. Ниже приведены наиболее часто используемые определения или определения, применяемые для данного исследования. В порядке упоминания:

- **Распределённый реестр** (distributed ledgers): распределенная база данных, хранящаяся на множестве узлов, записи в которой синхронизируются через механизмы консенсуса.
- **Блокчейн** (blockchain): наиболее распространенный механизм подтверждения консенсуса в распределенных реестрах. Часто используется как синоним для распределённых реестров в целом.
- **ICO** (Initial Coin Offering): первичное размещение токенов, в ходе которого проекты привлекают средства путём продажи цифровых токенов, предназначенных для последующей оплаты услуг блокчейн платформы площадки.
- **Токены \ Utility токен**: проприетарная цифровая валюта для оплаты продукта или услуг блокчейн проекта.
- **Смарт-контракт** (smart contract): программный код, в котором формулируются условия ICO и функционал токена.
- **White paper**: документ проекта, выходящего на ICO, с описанием проекта для инвесторов.
- **KYC** (Know Your Client, Знай Своего Клиента): процедура подтверждения личности покупателя токена.
- **Баунти программы**: распределение токенов на специальных условиях ограниченному кругу первых инвесторов.
- **Открытый блокчейн** (public/permissionless blockchain): участником блокчейн может стать кто угодно.
- **Закрытый блокчейн** (private/permissioned blockchain): участников блокчейн и их права (запись, просмотр, майнинг) определяет администратор.
- **Фишинг**: создание точных копий (клонов) сайтов с целью выманить данные пользователей.
- **Capped sale**: продажа токенов, при которой объем привлечений ограничен, и токены реализуются по фиксированной цене.
- **Uncapped sale**: продажа токенов, при которой объем не ограничен, токены распределяются по факту окончания ICO пропорционально инвестициям.