



**ТАШКЕНТСКИЙ УНИВЕРСИТЕТ  
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ  
ИМЕНИ МУХАММАДА АЛ-ХОРАЗМИЙ**

**ДИСЦИПЛИНА:  
«ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ»**

**САМОСТОЯТЕЛЬНАЯ РАБОТА**

**«Технология блокчейн в защите  
информации»**

**СТУДЕНТ: *Ходжаев Мардонбек.***

# План

- ▶ 1. Введение
- ▶ 2. История блокчейна и его применений в BitCoin
- ▶ 3. Блокчейн как структура данных
- ▶ 4. Надежность и перспективы блокчейна

# Введение

- ▶ Blockchain - это
  - ▶ 1. Технология учета и обмена правами собственности на цифровые активы в одноранговой сети (Одноранговой называется сеть, в которой основной упор является на равноправии участников, то есть децентрализации самой сети.)
  - ▶ 2. Структура данных, похожая на комбинацию массива и односвязного списка.

# Создание блокчейна

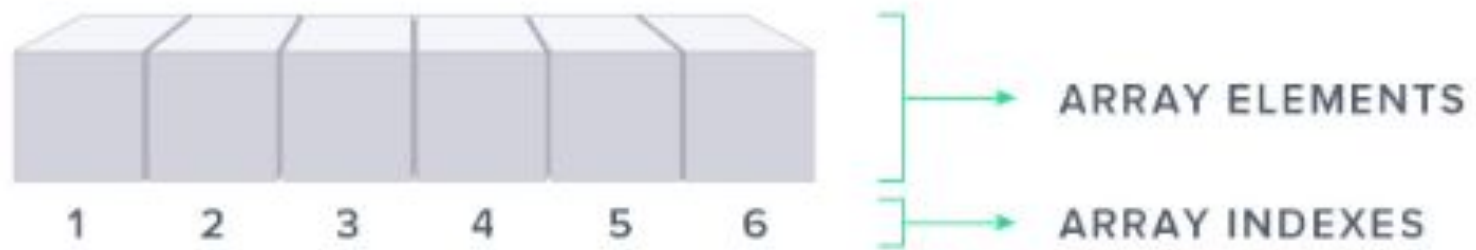
- ▶ 1983 - Были предложены первые протоколы “электронной наличности” (электронная наличность - средства платежа в электронном, безматериальном виде)
- ▶ 1997 - 1998 - Были предложены идеи HashCash, которые легли в основу процедуры создания новых блоков в биткойн-базе. Адам Бэк предложил идею о системе доказательства правильности работы, используемой в целях нейтрализации спама и DoS-атак. Позднее она будет использована в BitCoin и других криптовалютах, как часть алгоритма анализа данных.
- ▶ 2008 - Опубликован протокол и принцип работы платёжной системы BitCoin
- ▶ 2009 - Был сгенерирован первый блок и первые 50 биткойнов, а также проведена первая в истории транзакция по переводу биткойнов, а позднее обмен биткойнов на национальную валюту.

# Создание блокчейна

- ▶ 2010 - Первый обмен биткойнов на реальный товар (то есть первый случай использования биткойнов в качестве надёжной валюты)
- ▶ 2013 - Реализованы первые смарт-контракты на Блокчейне
- ▶ По разным источникам, считается что человек или группа людей под псевдонимом “Сатоши Накамото” разработали протокол криптовалюты биткойн, то есть в числе первых реализовавшие применение технологии блокчейна.

# Что такое блокчейн?

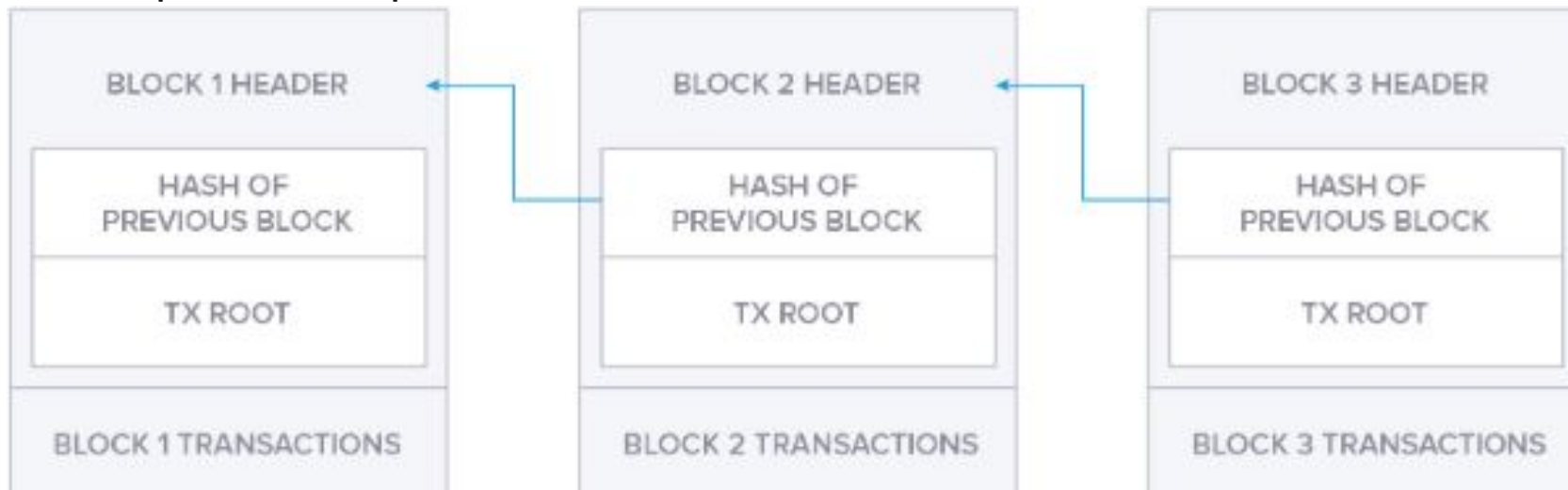
- ▶ Блокчейн как структура данных:
  - ▶ Блокчейн является неким результатом слияния массива и связанного списка



Массив

# Что такое блокчейн?

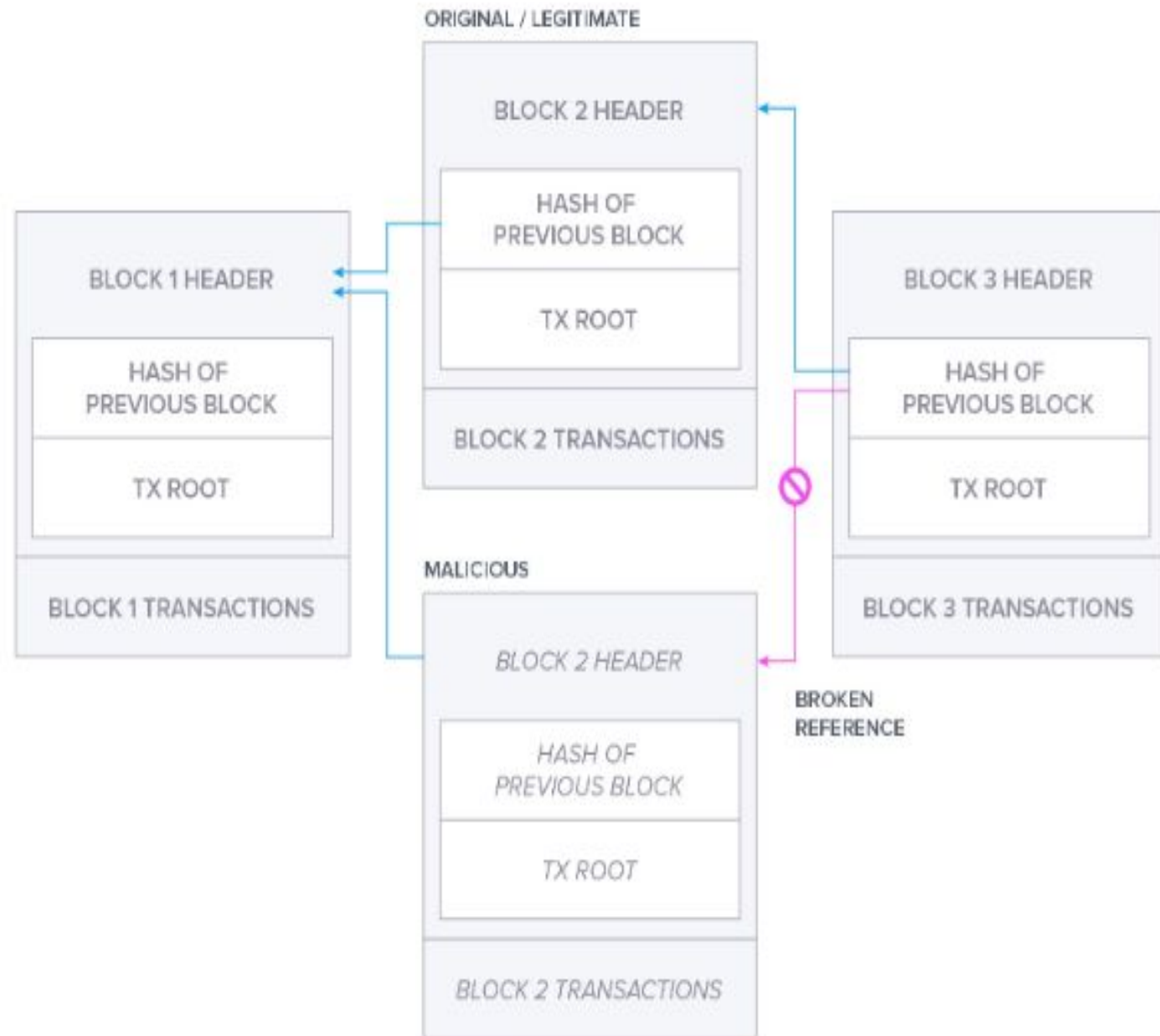
- ▶ В контексте структур данных блокчейн наиболее напоминает связный список. Также в блокчейне данные разделяются по контейнерам, именуемым *блоками*. Блоки вполне аналогичны *узлам* связного списка. В каждом блоке содержится ссылка, представляющая собой хэш предыдущего блока. Она служит связкой с предыдущим блоком и помогает поддерживать порядок в цепочке блоков.



Визуализация блокчейна

# Отличие блокчейна от связанного списка

- ▶ Ключевое отличие между блокчейном и связным списком заключается в том, что каждая ссылка в блокчейне криптографически защищена. Возможно, вы слышали применительно к блокчейну термин «append only» — «только для добавления». Он означает, что вносить новые данные в блокчейн можно, лишь достраивая цепочку спереди. Валидность защищенных связей постоянно проверяется. Если бы можно было вставить в середину блокчейна вредоносный блок, например, между блоками 1 и 3 на схеме ниже, то можно было бы поставить ссылку на предшествующий ему блок 1, но не на следующий за ним блок 3.



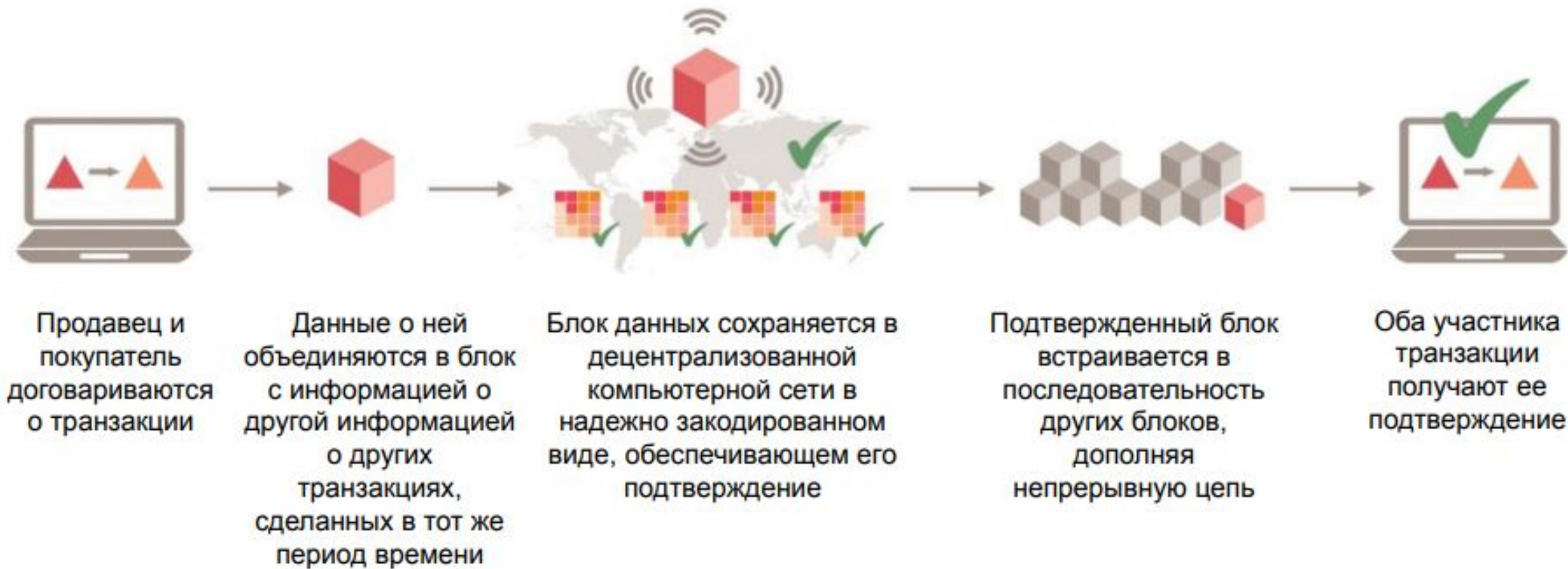


# Надежность структуры блокчейн

Каждый новый блок надстраивается над уже имеющимся, и такая процедура обычно именуется подтверждением. Чем старше блок, тем больше подтверждений у него будет. Каждое подтверждение осложняет подделку данных в блоке. На следующей схеме у блока 2 одно подтверждение. Чтобы подделать данные в блоке 2, вам придется воссоздать один валидный блок, в котором будет новая валидная ссылка. После каждого следующего подтверждения придется воссоздавать еще один блок. Таким образом, чем старше блок, тем выше уверенность, что никаких изменений в этот блок внесено не будет.

Ссылки между блоками зависят не только от порядка блоков, но и от того, какие данные содержатся в каждом блоке. Невозможно добавить или удалить данные из блока в блокчейне. Именно на этом свойстве базируется уверенность, что с данными, помещенными в блокчейн, ничего не случится. Естественно, в структуре данных блокчейна любая подделка очевидна. Любое изменение, вносимое в данные, ломает ссылки на все последующие блоки.

# Как это работает на практике?



# Перспективы блокчейна

Технология блокчейн решает ряд проблем, среди которых можно выделить следующие:

- Защита прав собственности
- Защита авторских прав
- Удешевление и ускорение денежных переводов
- Монетизация и защита персональных данных
- Сокращение транзакционных издержек
- Устранение асимметрии информации
- Повышение доверия



**СПАСИБО ЗА ВНИМАНИЕ !**