# Разработка децентрализованной платежной системы на основе технологии blockchain с учетом специфики мобильных платформ

Илюхин А.А[1], Никонов Э.Г[2]

[1]ГБОУ ВО МО «Университет «Дубна», Институт системного анализа и управления.

[2]Лаборатория информационных технологий, Объединенный институт ядерных исследований

GRID 2018, Дубна, 10-14 сентября

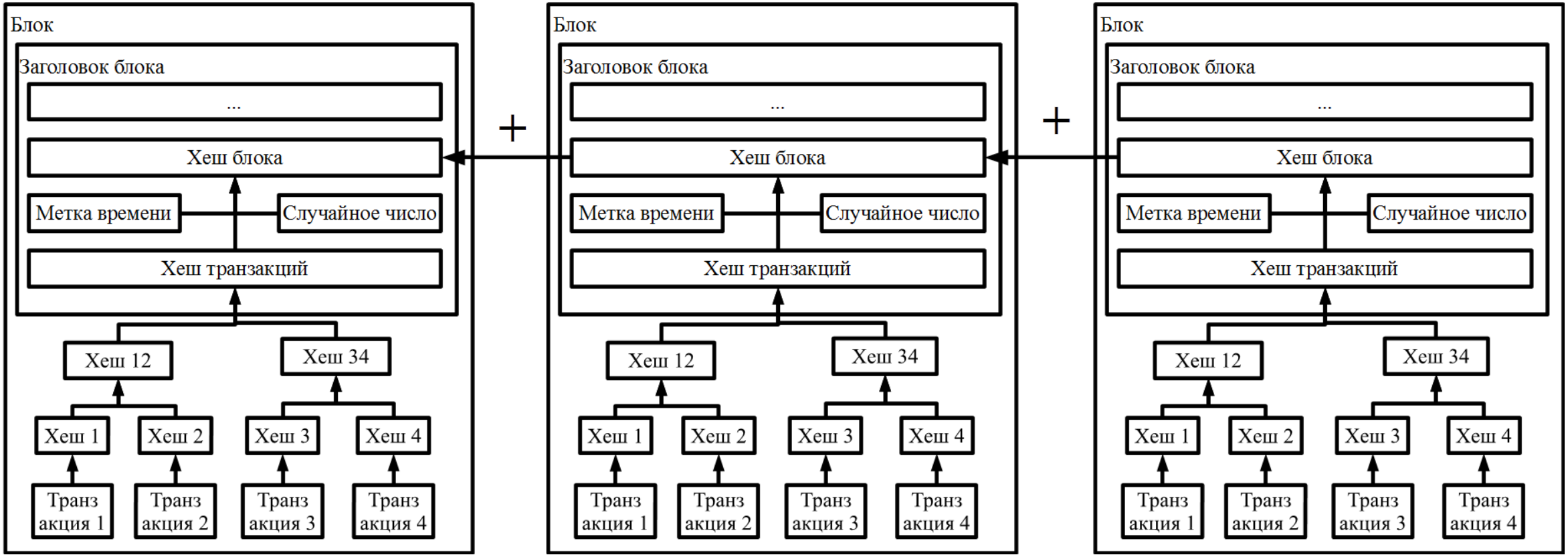
# Задачи

На пути интеграции мобильных платформ в сферу blockchain имеются следующие сложности:

- Масштабируемость.
- Ненадежность консенсусов.
- Необходимость хранить большие объёмы данных.
- Угроза со стороны квантовых вычислений.
- Конфиденциальность.

В данном докладе будут рассмотрены решения для первых трех задач.

# Технология Blockchain



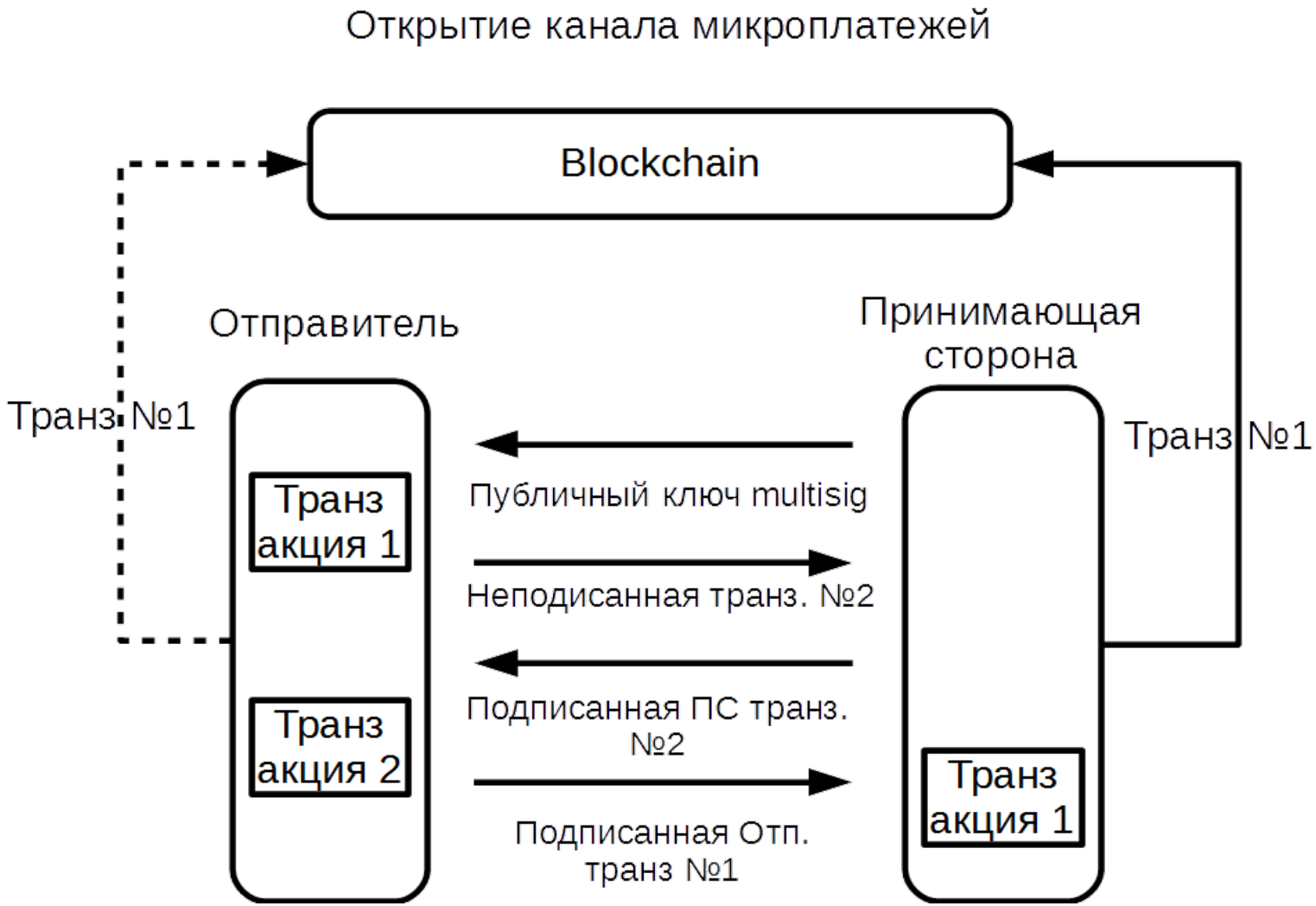
# Виды консенсусов

- Proof-of-Work (Pow) – «доказательство выполненной работы».
- Семейство «Доказательство доли владения»:
  - Proof-of-Stake (PoS).
  - Delegated Proof-of-Stake (DpoS).
  - Leased Proof-of-Stake (LpoS).
- Гибридные:
  - Proof-of-Burn (PoB) – «доказательство сжигания».
  - Proof-of-Activity (PoA) – «доказательство активности».
- Proof-of-Capacity (PoC) – «доказательство ресурсов».
- Proof-of-Importance (PoI) – «доказательство значимости».
- Proof-of-Authority (PoAuthority) – «доказательство полномочий».

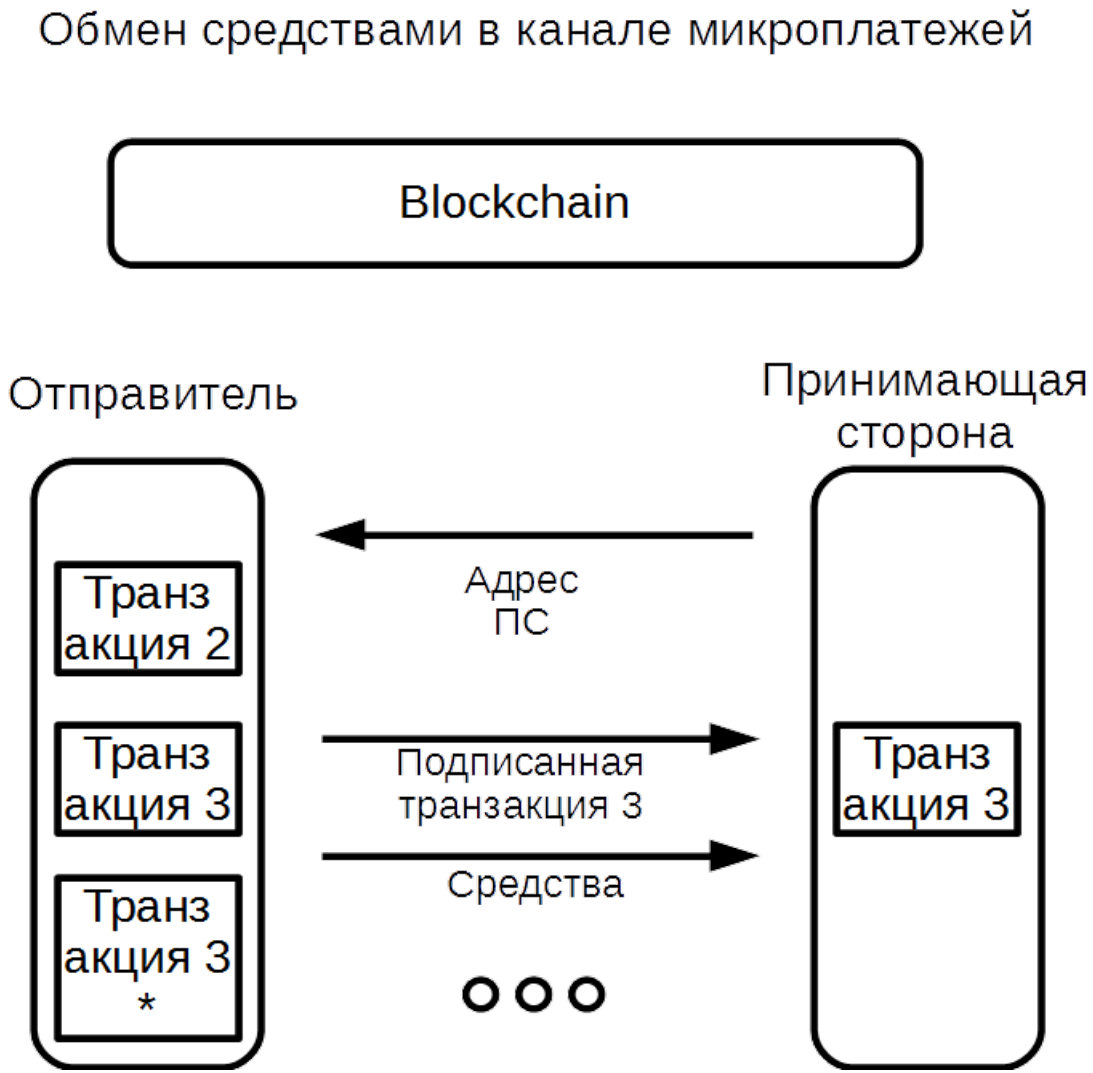
# Подходы к решению проблемы масштабируемости

- Каналы микроплатежей
- Sharding
- Направленные ациклические графы

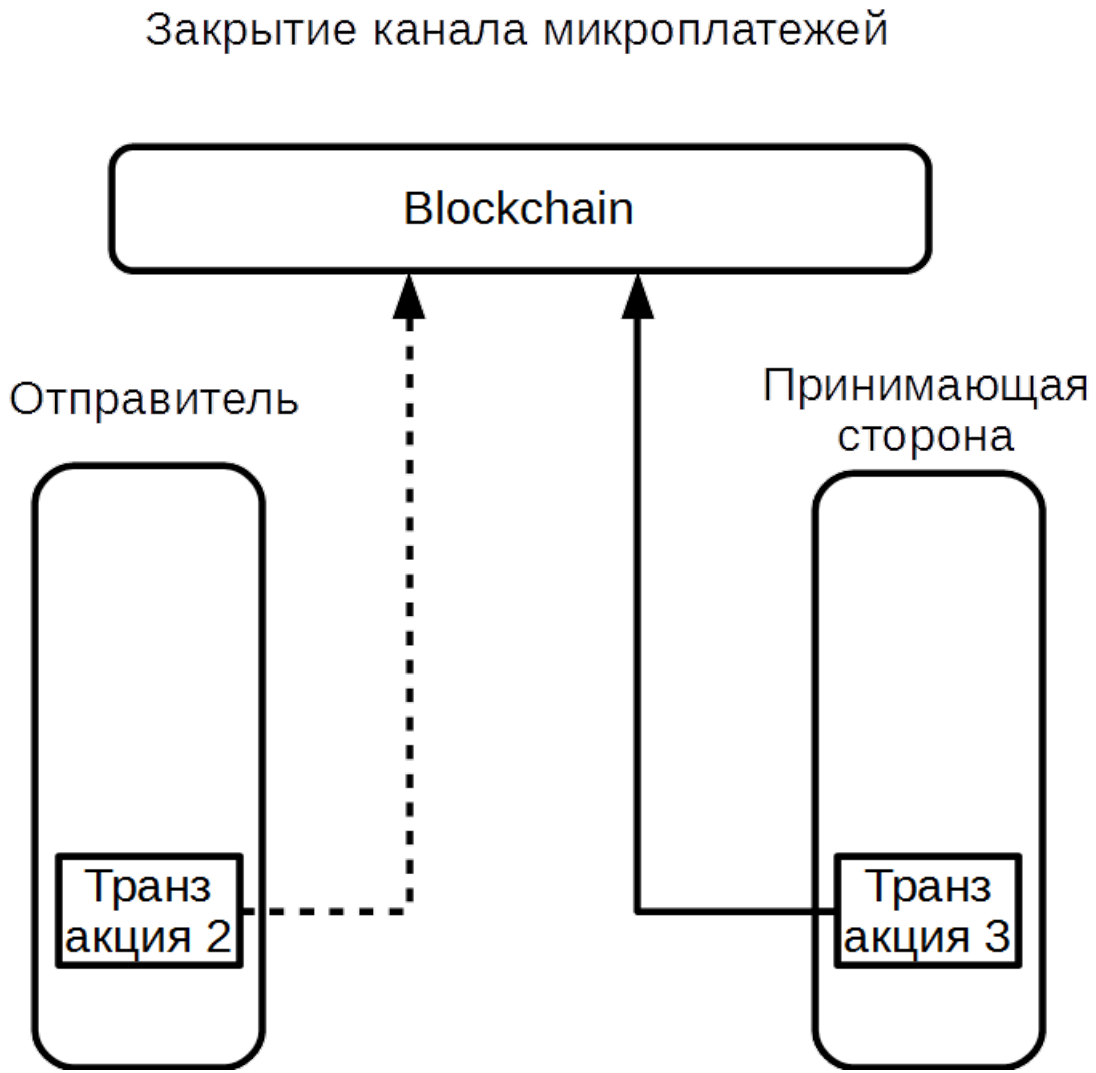
# Каналы микроплатежей



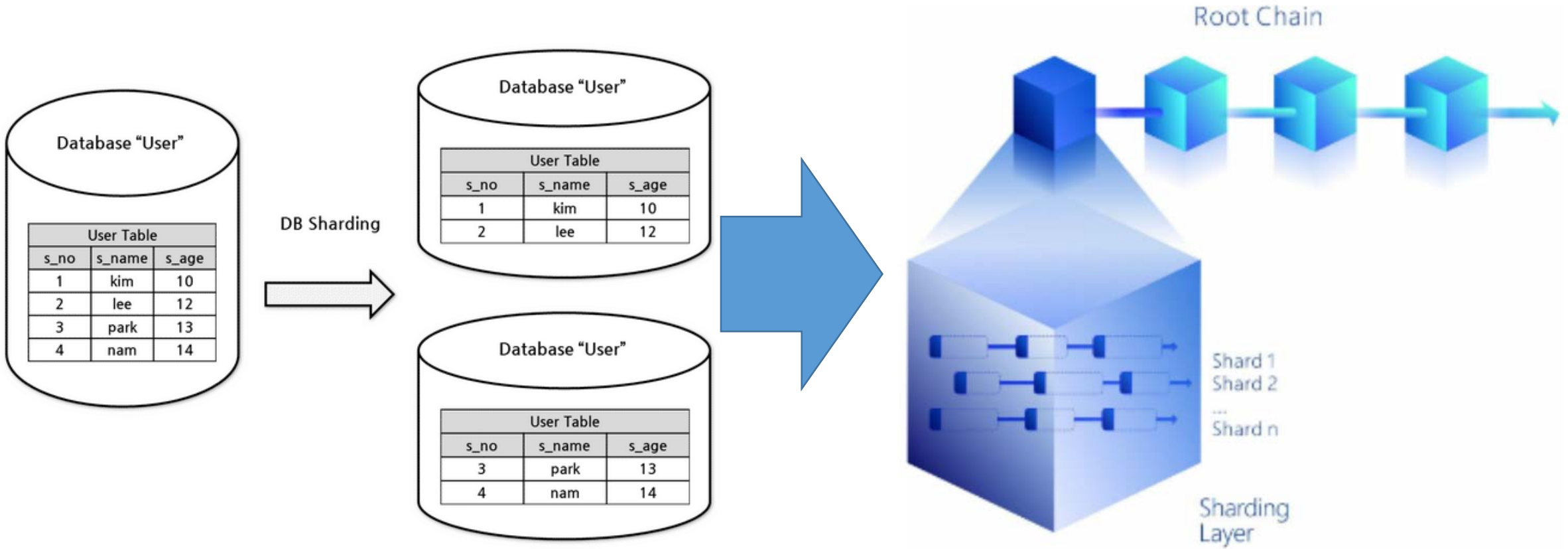
# Каналы микроплатежей



# Каналы микроплатежей



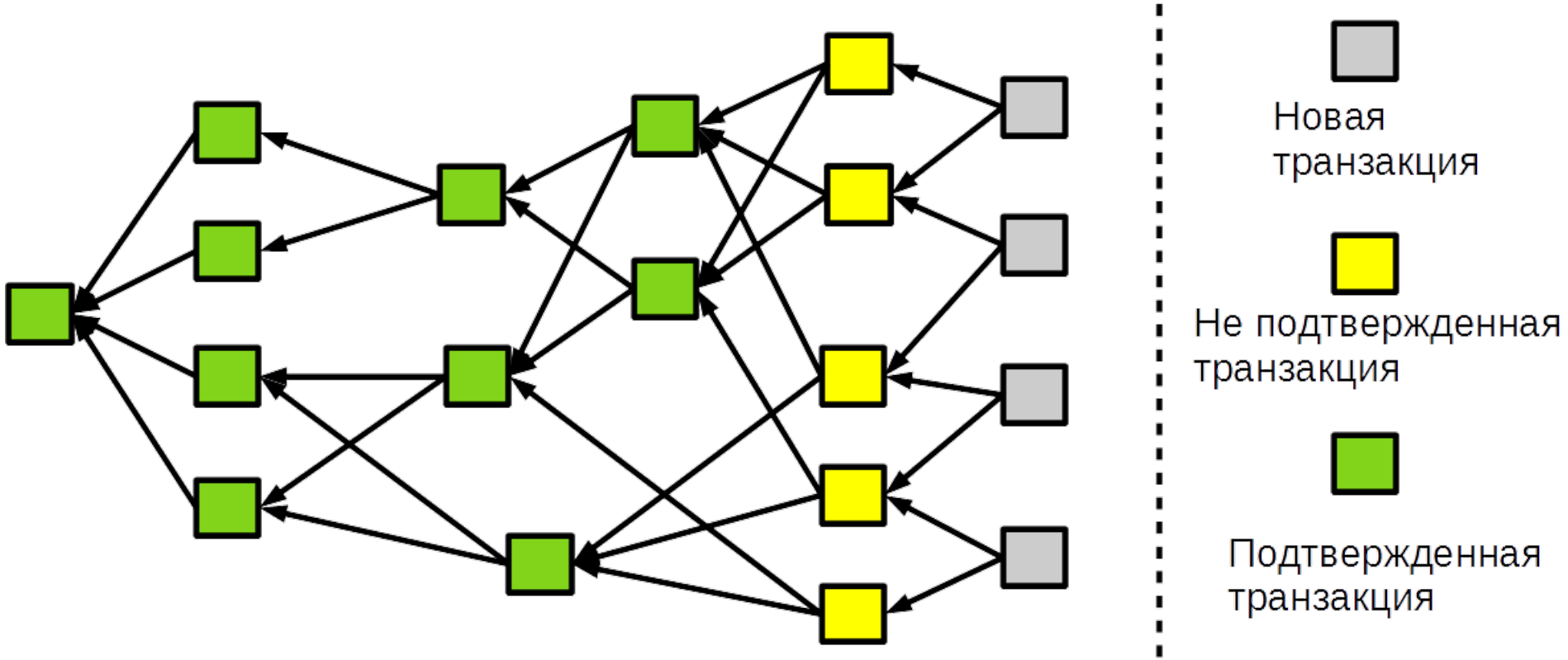
# Sharding




Sharding баз данных

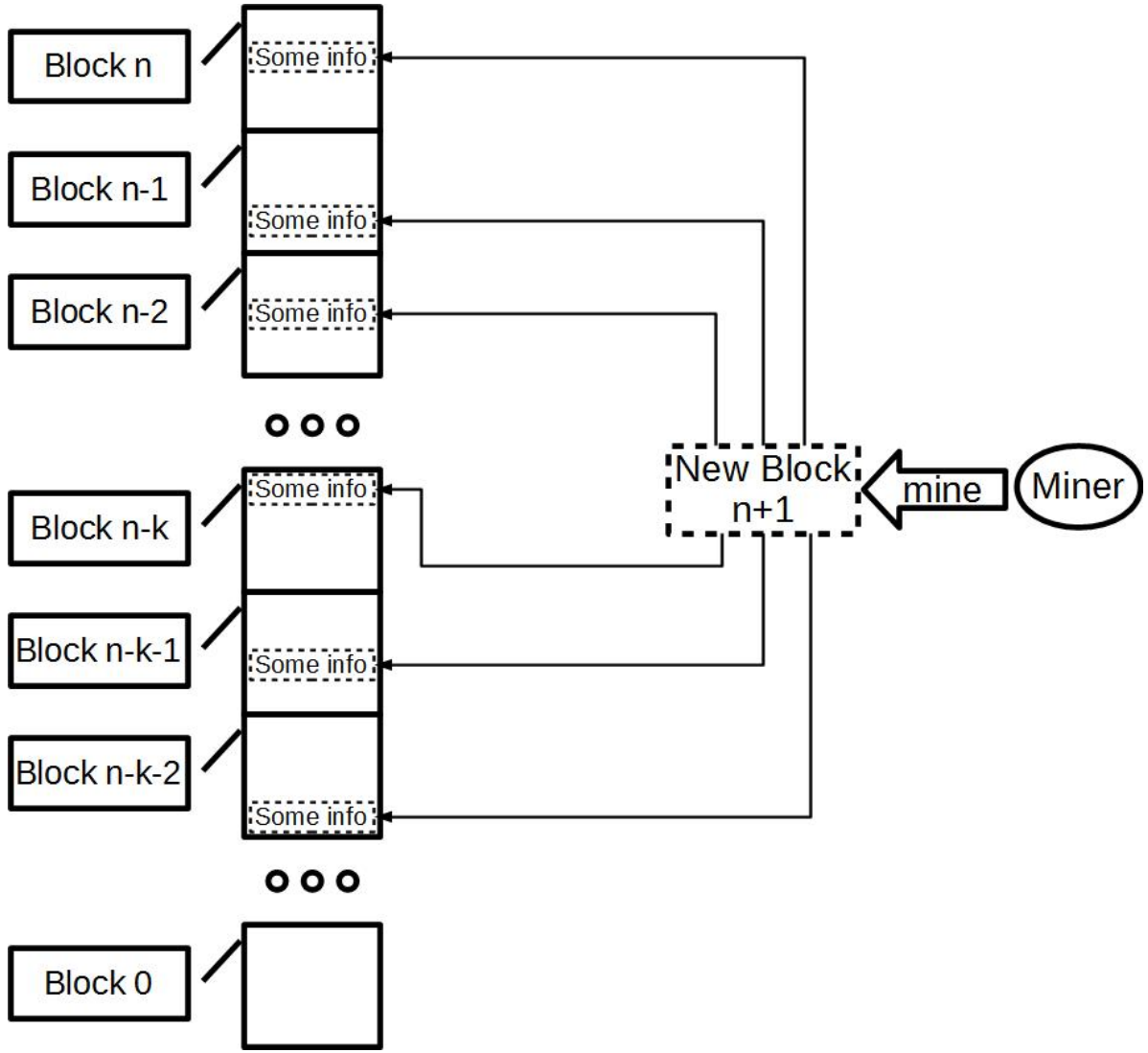
Sharding blockchain

# Направленные ациклические графы (IOTA)

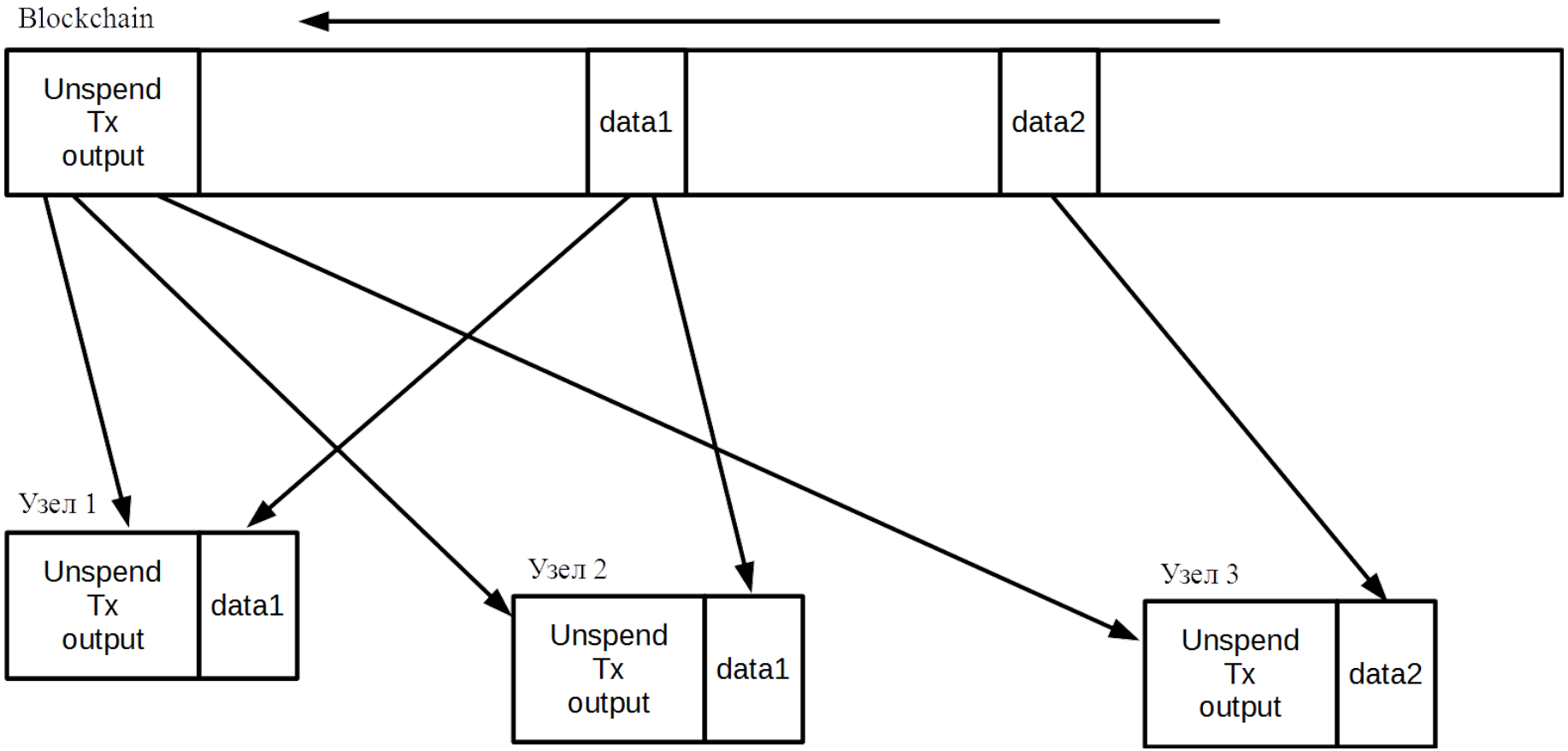


# Разработка консенсуса

Схема генерации блока в доработанном варианте Proof-of-Stake.



# Предложения по решению проблем масштабируемости




Концепт организации хранения blockchain на узлах сети.

# Спасибо за внимание!