Платформа и криптовалюта IOTA

Антонова Анастасия, БПИ182

История создания IOTA

Идея: создать платформу для транзакций между устройствами IoT.

Проект IOTA был основан в **2015** году в Германии Дэвидом Сэнстебё, Сергеем Иванчегло, Домиником Шинером и Сергеем Поповым. В середине **2017** IOTA вышла на биржу криптовалют.

Координирует разработку экосистемы IOTA некоммерческая организация IOTA Foundation

Общее количество монет: 2,779,530,283,277,761 iota

Преимущества

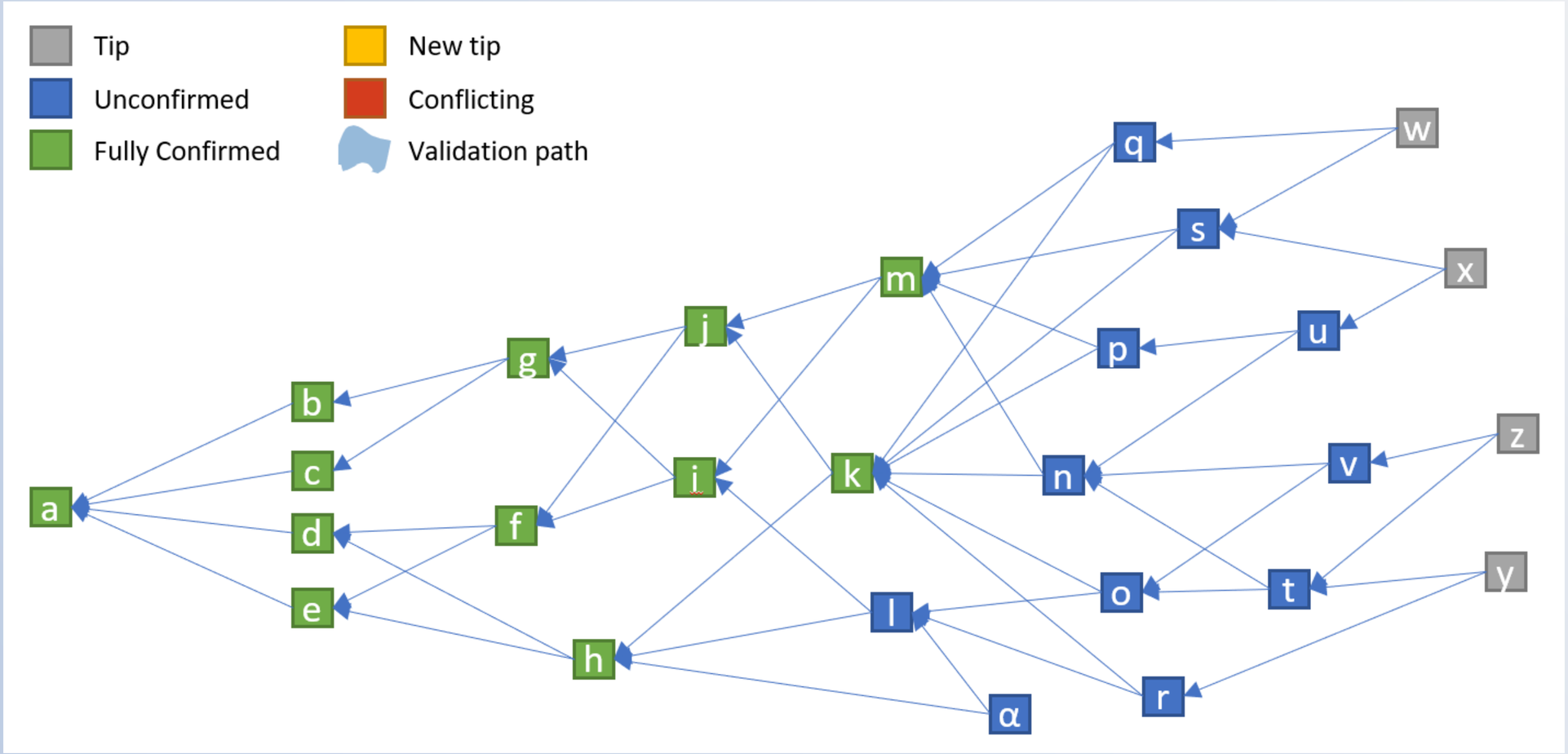
- Бесплатные и быстрые транзакции
- Возможность проводить микротранзакции
- Количество одновременно обрабатываемых транзакций не ограничено
- Система легко масштабируется

Tangle

Технология консенсуса на основе направленного ациклического графа (DAG).

Вершина графа — транзакция, она содержит информацию об отправителе, получателе, сколько монет переводится и ссылки на другие транзакции.

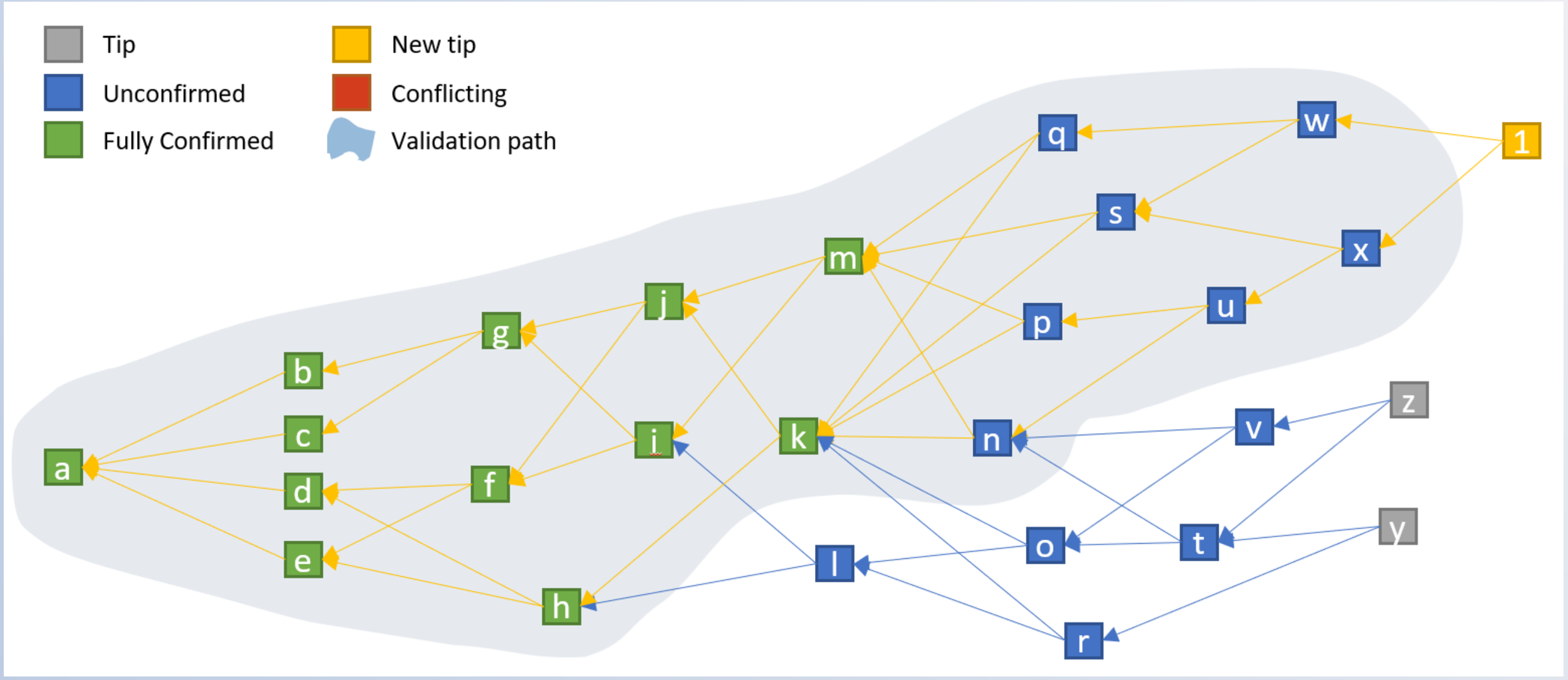
Tangle


Tip
Unconfirmed
Fully Confirmed
New tip
Conflicting
Validation path
a
b
c
d
e
g
f
h
j
i
m
k
l
α
q
s
p
n
o
r
w
x
u
v
t
z
y

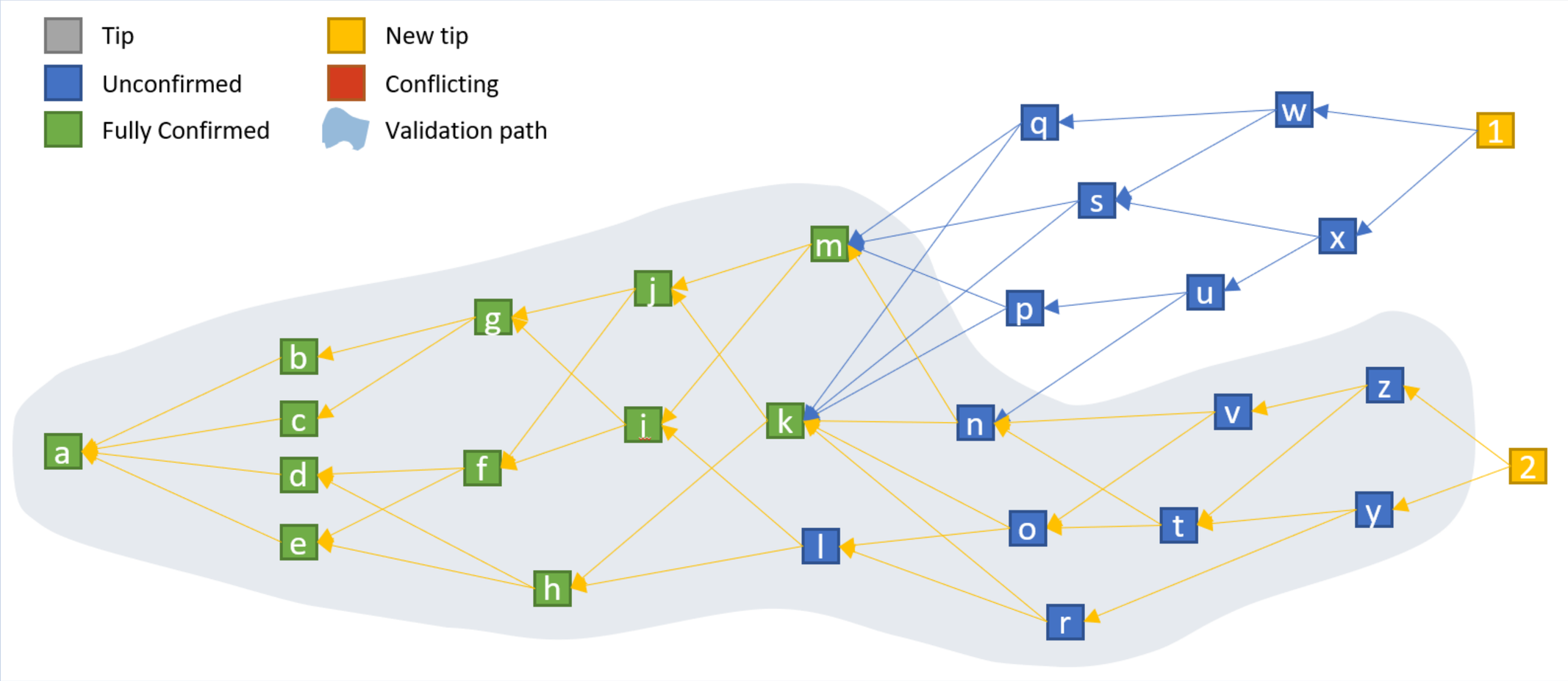
Как добавить транзакцию?

- Найти две случайные неподтвержденные транзакции (tips)
- Валидация этих транзакций: проверить цифровую подпись, их PoW, есть ли конфликты между транзакциями в этой части графа (double spending)
- Если валидация пройдена, то новая транзакция добавляется в Tangle, ссылаясь на них
- Если нет, то выбираются две другие случайные tips
- Транзакции, которые подтверждены всеми или почти всеми текущими tips считаются полностью подтвержденными

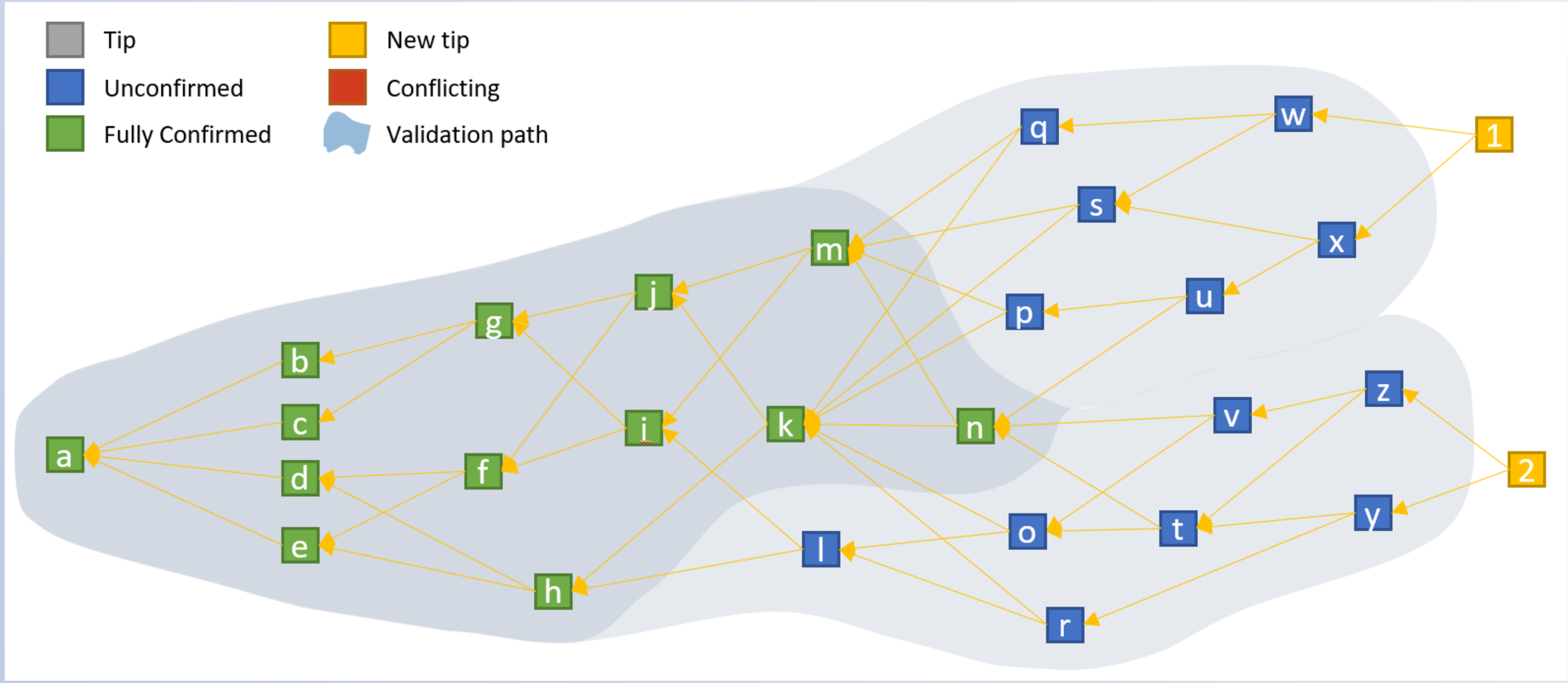
Как добавить транзакцию?



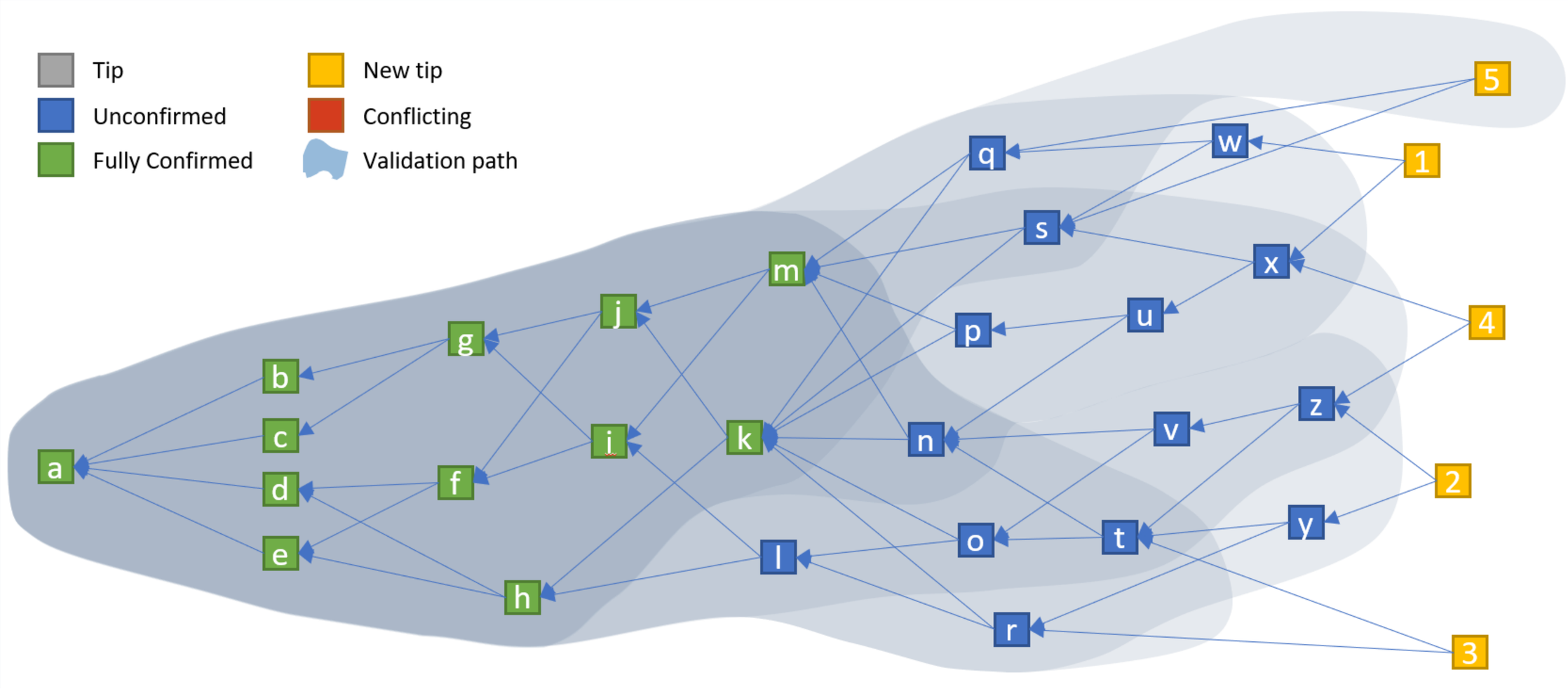
А еще одну?


Tip
Unconfirmed
Fully Confirmed
New tip
Conflicting
Validation path
a
b
c
d
e
f
g
h
i
j
k
l
m
n
o
p
q
r
s
t
u
v
w
x
y
z
1
2

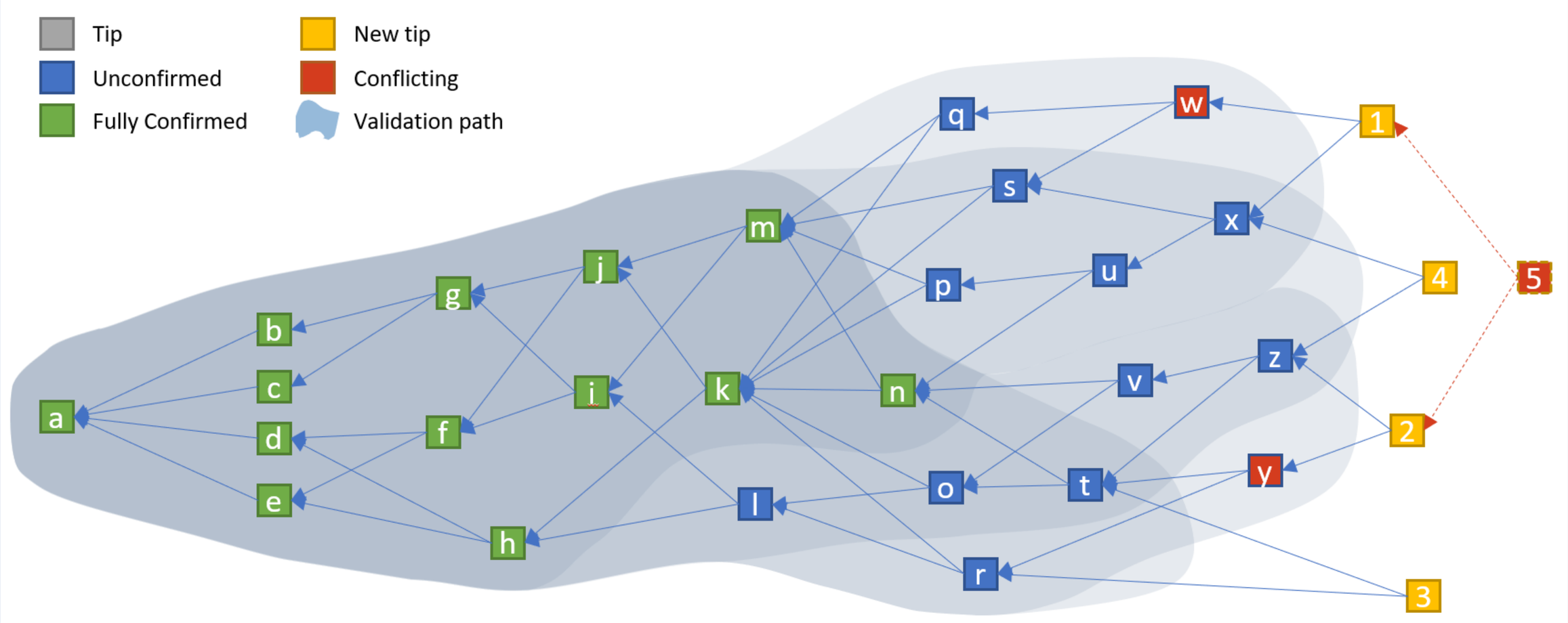
Новое состояние Tangle



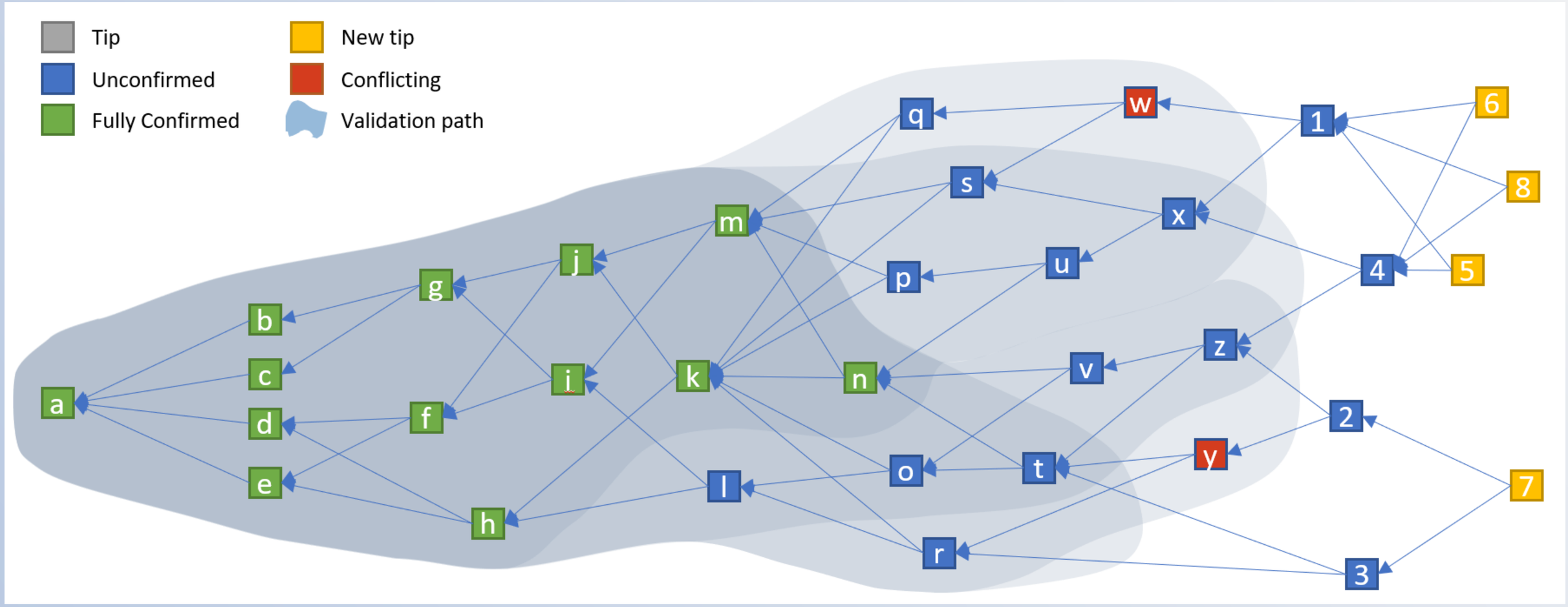
Добавим еще транзакций



Конфликтующие транзакции



Конфликтующие транзакции



Подтвержденные транзакции

Разработчик сети на основе IOTA может выбрать уровень доверия транзакции — какая доля tips должна ссылаться на транзакцию, чтобы она считалась подтвержденной, например, 99%. Технология называется Fast Probabilistic Consensus.

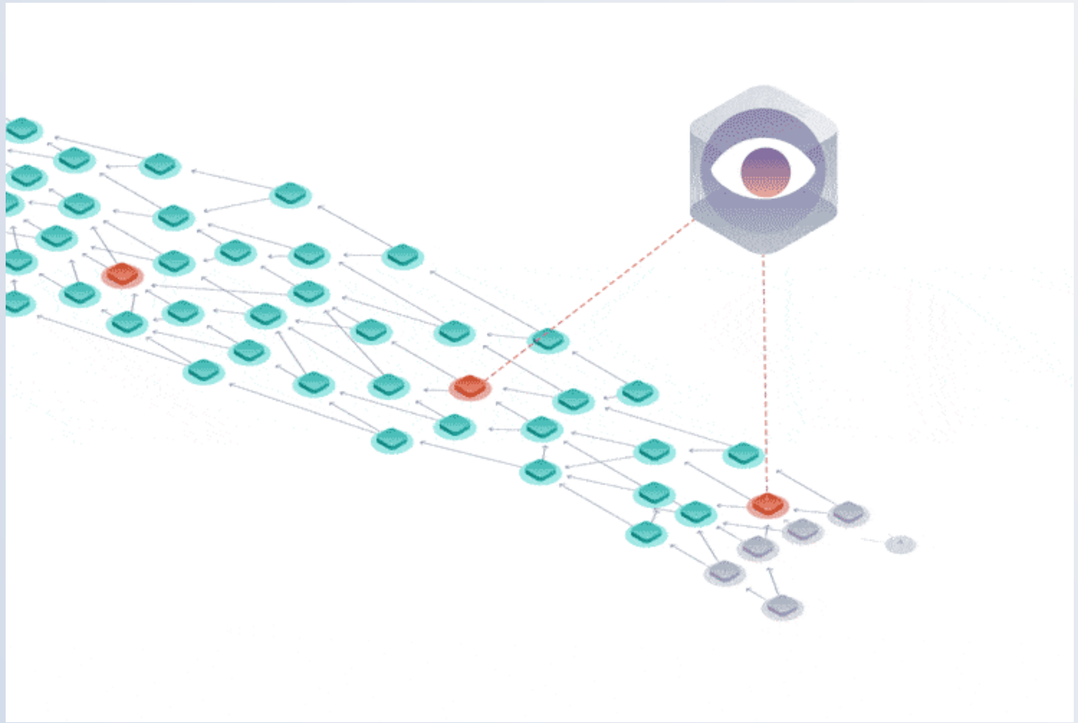
Она уязвима для атаки 51%, но сейчас используется вместе с Координатором для подтверждения транзакций.

Так как PoW не используется для подтверждения транзакций, время- и энергозатраты очень малы.

Координатор

Сейчас в сети есть особый клиент — координатор. Это временное решение, его уберут в IOTA 2.0.

Транзакции в Tangle считаются подтвержденными, только если на них ссылается напрямую или не напрямую milestone — подтвержденное другими транзакциями сообщение от координатора.



Криптография

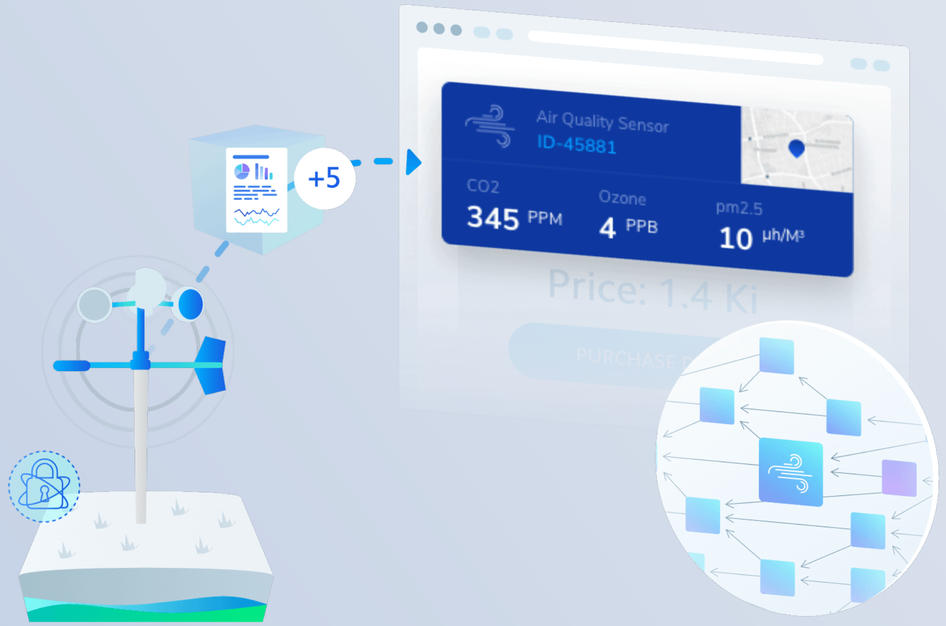
В IOTA используются криптографические подписи, основанные на хешировании Winternitz, вместо эллиптической криптографии (ECC). Подписи на основе хеширования значительно быстрее, нежели ECC.

Как завести кошелек (M)IOTA?

Пользователь нового кошелька должен самостоятельно создать секретную фразу длиной до 81 символа, используя заглавные латинские буквы и цифру 9. Эта секретная фраза используется для генерации приватных ключей и обеспечивает доступ к кошельку с любого устройства.

Data Marketplace

На основе IOTA был открыт публичный рынок для данных, предоставляемых сторонними датчиками. Он позволяет подключённым устройствам безопасно передавать, покупать и продавать кому угодно небольшие объемы разнообразных данных.



Список источников

1. IOTA Wiki — https://wiki.iota.org/learn/about-iota/an-introduction-to-iota

2. IOTA Transactions, Confirmation and Consensus — https://github.com/noneymous/iota-consensus-presentation

3. IOTA (технология) — https://ru.wikipedia.org/wiki/IOTA_(технология)