IOTA

Meetup #2

Deep Dive on IOTA & Tangle

Event Organizers

dcentrum Community

Connect | Collaborate | Create

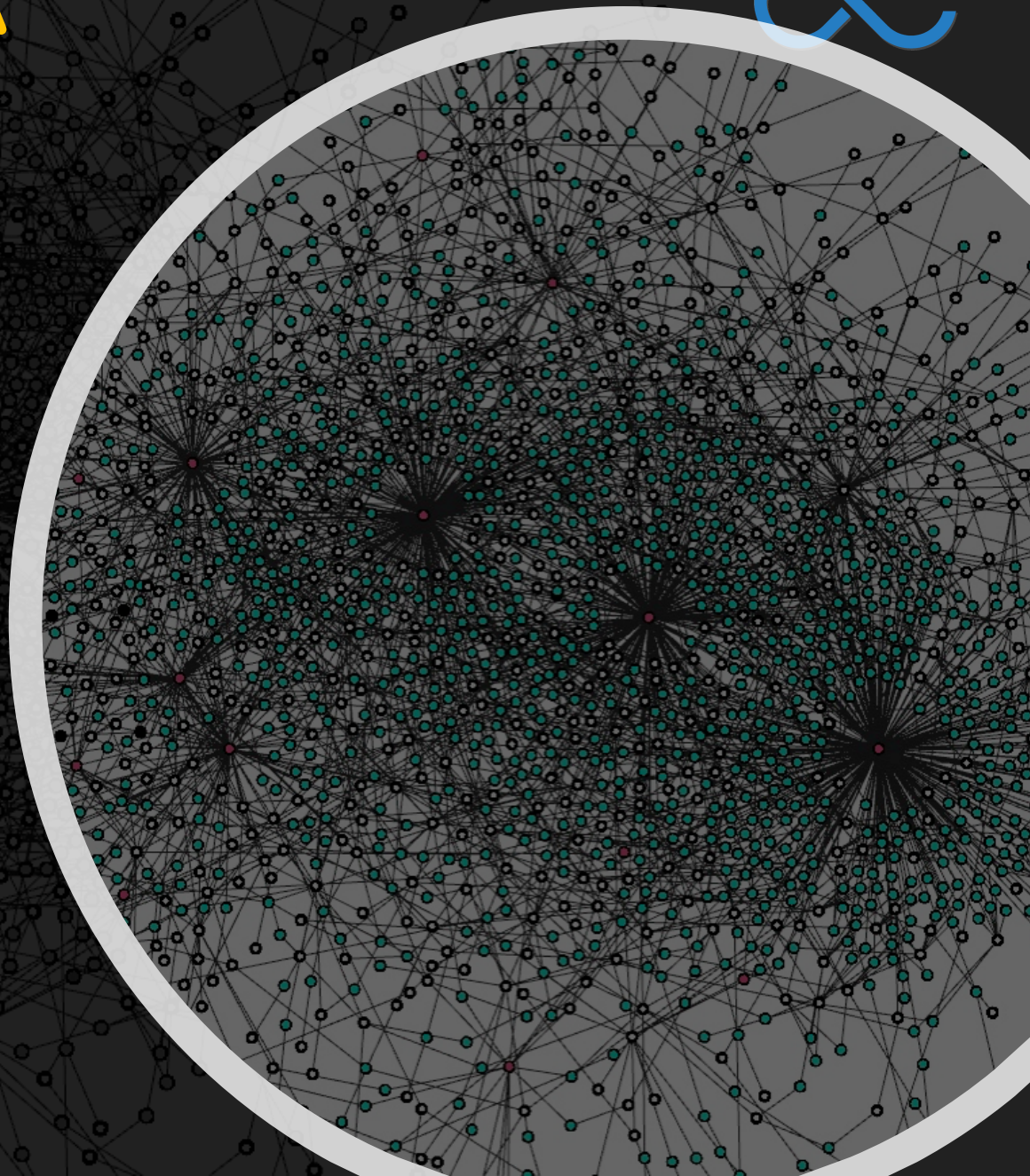
Event Supporters

nagarro.

THINKING BREAKTHROUGHS

Meetup #2 – Foundations of IOTA

- How does IOTA work?
  - Tangle, Trytes, Seeds, Addresses, Transactions, Bundles, Nodes, MAM
- Directed Acyclic Graphs and Tangle - Deep Dive
  - What is DAG and its importance
  - how does tip selection occur
  - how are malicious transactions avoided
  - Transactions, Consensus and Proof of Work on Tangle
- IOTA Tokens and Trinity Wallet
  - how to get test tokens on devnet
- Playing IOT Hardware and Devices
  - connecting them to IOTA



DCentrum's 4-month Blockchain co-learning series:

IOTA

Join to experience perfect way to learn and solve real world problems using IOTA Tangle with a group of highly motivated Decentralization enthusiasts

registration

http://bit.ly/IOTAHydMeetups

** Venue will be announced via Slack and confirmations after curation based on responses on above form

Hyderabad, India

Meeting Frequency
Bi-Weekly

Total Series Duration
3 Months

23 March 2019 – 6 July 2019

First thru Third Meetings:

- ✓ **Level Setting**
- ✓ **Foundation**
- ✓ **Concepts**

During initial two meetings we all will get to know each other and understand the foundational aspects to **Tangle** & **IOTA**. How is it different from Blockchain. Learn to document a use-case and Business Model.

Bring together and build a solid foundation

Fourth Meeting:

- ✓ **Real World use case selection**
- ✓ **Architecture, Scope Decisions**

Members will propose ideas to implement and we will together pick one or more use cases by looking at domain expertise and interest from majority of the participants. Idea(s) selected will provide choice to members to form groups and brainstorm about the scoping and architecture for the use case.

Encourages ideation and innovation from community

Fifth thru Seventh Meetings:

- ✓ **Building Solution by collaboration**

During this 45 day period we all will participate to build the end-to-end solution that will enable everyone coming together to build the chose use case(s)

Put the big picture in view and encourage team members to play various roles

Conclusion Workshop:

- ✓ **Condensed Version Workshop**
- ✓ **Showcase of Solutions built**

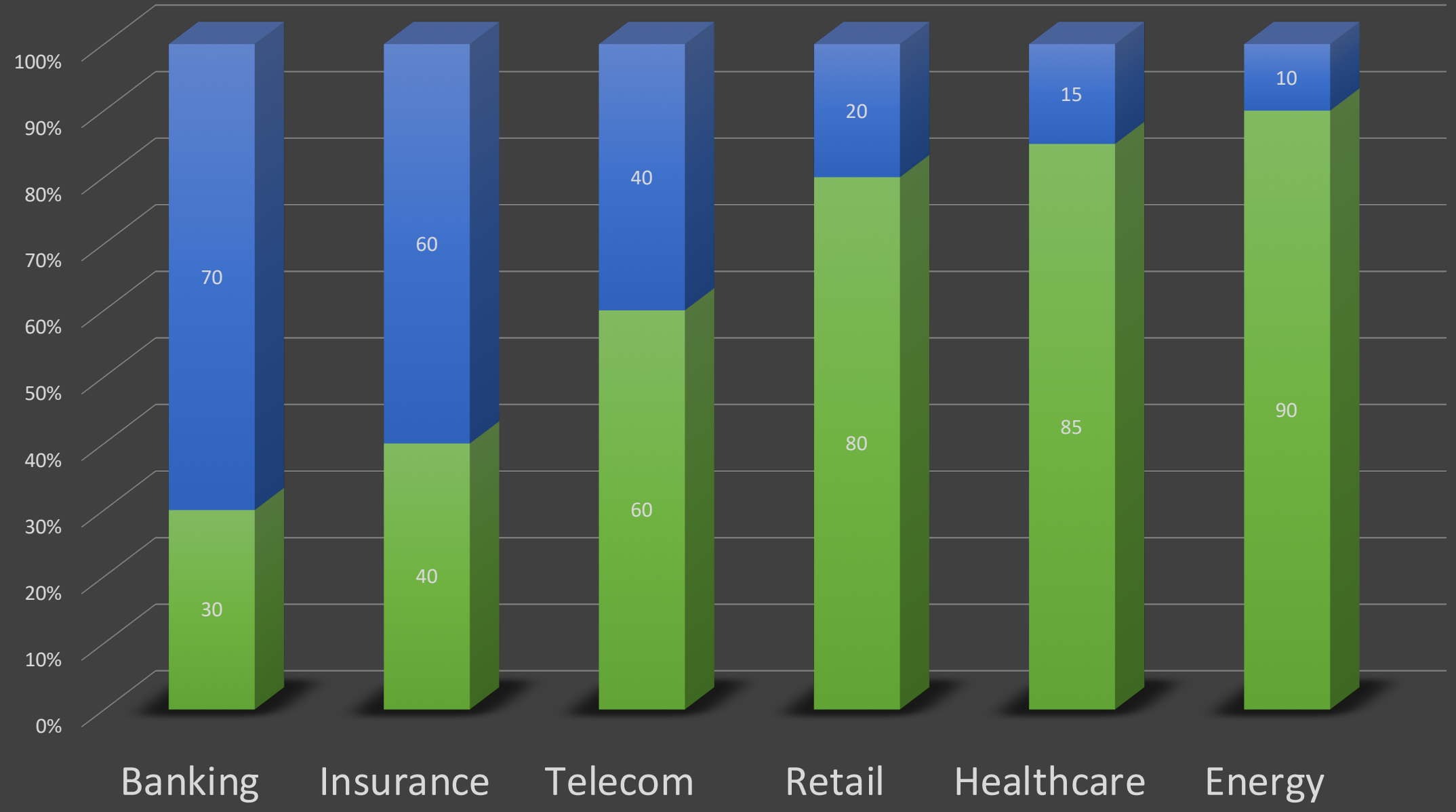
One day workshop for the open community to learn in a condensed approach what was done over a period of 3 months.

During this workshop, the ideas built will be showcased to the open community to help increase the connect and spread the idea.

Typical format of each meeting:

- Welcome & General Discussion [30 mins]
- 2 Presentations from members [30 min each]
- Shared Learning & Discussion [60 min]
- News Briefs [10 min]
- Open Discussion & Networking [20 min +]

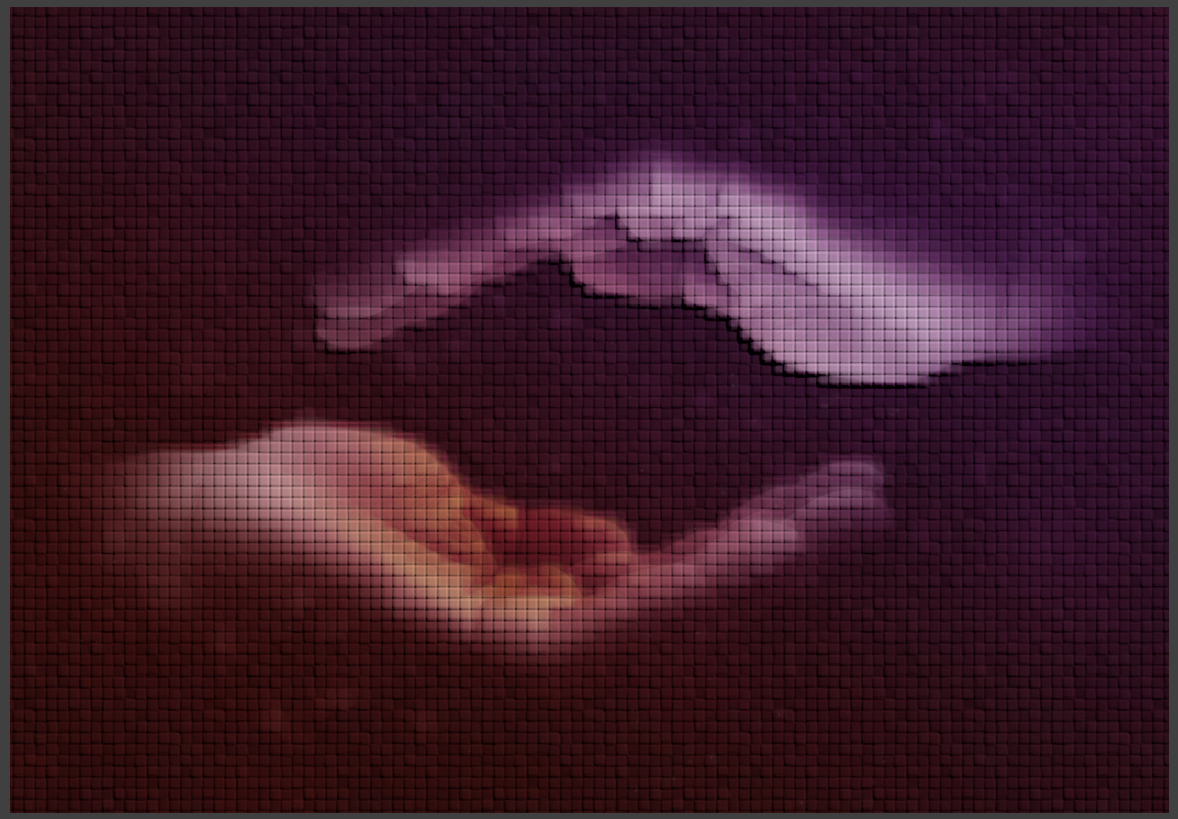
Physical vs Digital nature of transactions in various industries



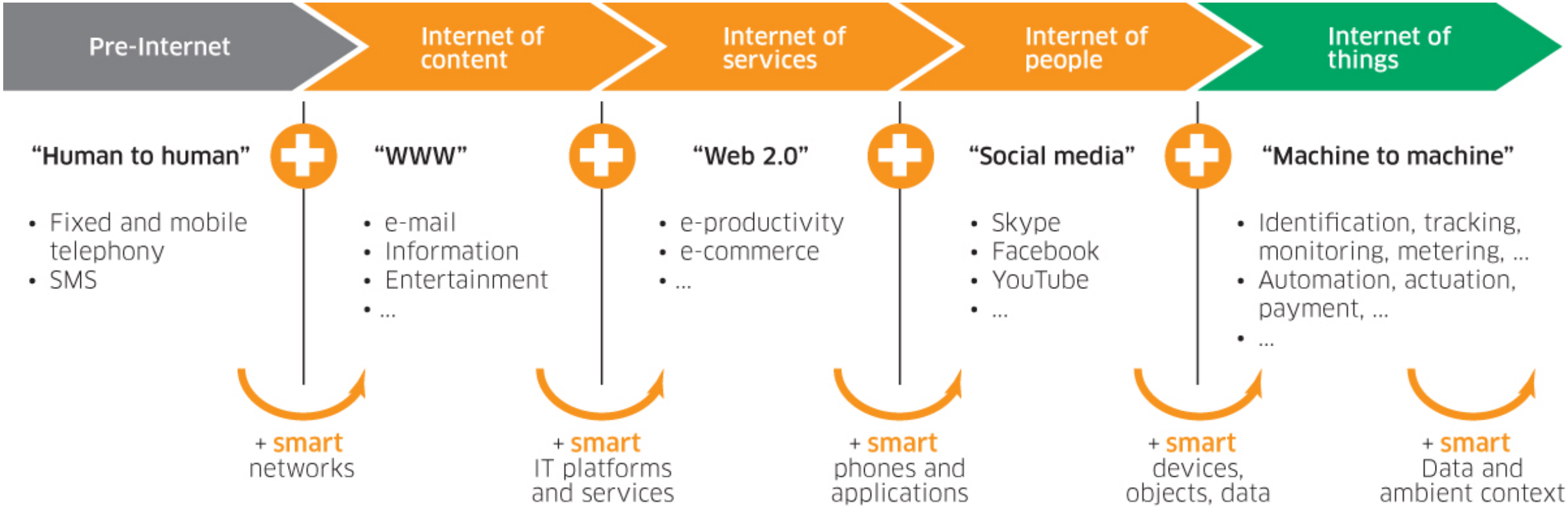
*Data shown for indicative purposes only

Blockchain is Blind!

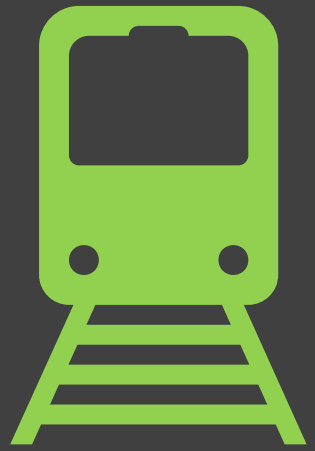
- As data becomes the new oil , trust in data is depleting
- Manual data entry is prone to collusion leading to mistrust
- So we need mechanisms that can help increase this trust in data, the saviours of such situations are:
  - Distributed Ledger Technology
  - Internet of Things
  - Machine Learning & Computer Vision



Evolution of Internet of Things



IoT Around us



Machine to Machine Payment – A Possiblity

Give 100 iotas

Name :Tessie

Requires an IOTA wallet which is recognized by a SEED

Requires minimum number of IOTA’s in the wallet

Name : ECCS

Requires an IOTA wallet which is recognized by a SEED

STEP1:

Tessie creates a Bundle

- SEED
  - Addresses & Private Keys (Kecccak – 384 hashing)
- BUNDLE
  - Group of Transactions
  - Tail Transaction / Head Transaction
  - Branch Transaction/ Trunk Transaction
  - Bundle Hash
  - Index

STEP 2

Tessie sends it to a Node for Validation

- TIP SELECTION
  - MCMC
  - Cumulative Weights
- Bundle Validation / Ledger Validation

STEP 3

Node Validates and add it to the Tangle

- CONFIRMATION CONFIDENCE
- CO-ORDINATOR

IOTA

Meetup #2

Directed Acyclic Graphs in IOTA Tangle

Event Organizers

dcentrum Community

Connect | Collaborate | Create

Event Supporters

nagarro.

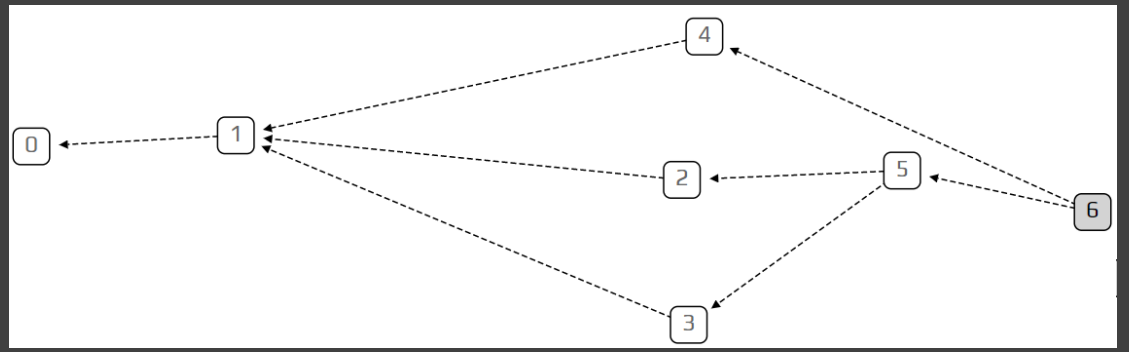
THINKING BREAKTHROUGHS

DIRECTED ACYCLIC GRAPH

DAG is a type of distributed ledger technology that relies on consensus algorithms. Consensus algorithms operate in a way that transactions that prevail simply require majority support within the network.

Directed Acyclic Graph - Tangle

- **Directed Graph**: Collection of vertices and Edges
- **Tangle**: Graph which holds transactions. Data Structure behind IOTA
  - **Vertex**: Transactions
  - **Edges**: Approvals
  - **Tips**: Unapproved Transactions
- When new transaction joins Tangle, it chooses 2 previous transactions (tips) to approve
- Strategy of choosing these 2 tips to approve is very important and key to IOTA's new technology

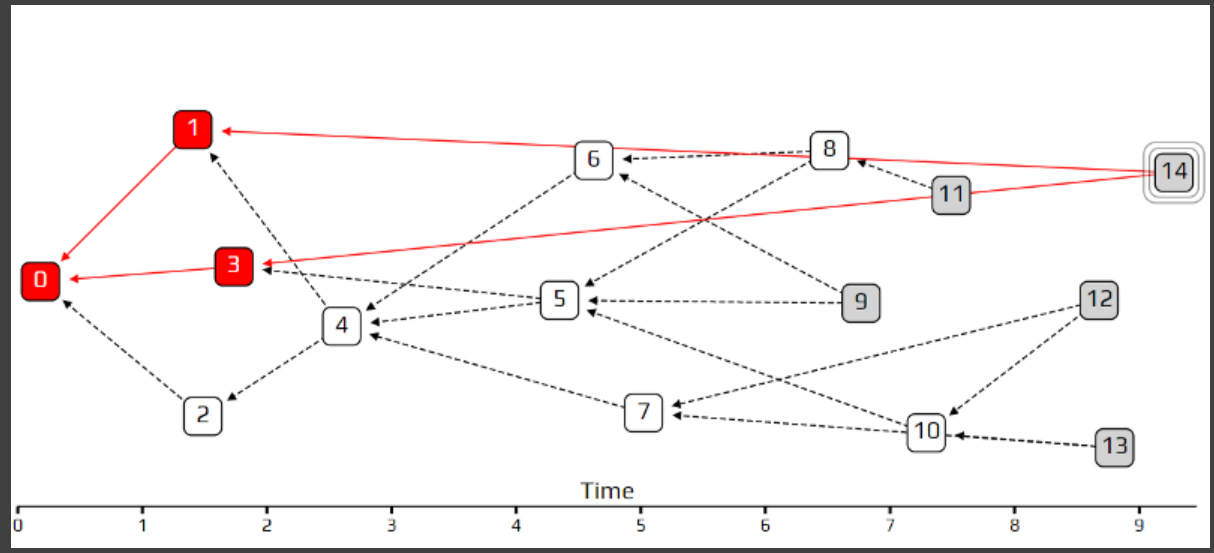


Directed Acyclic Graph

Tip Selection Algorithms

1. Uniform Random tip selection
   Simulation: https://public-rdsdavdrpd.now.sh/
2. Un-weighted Random walk
   Simulation: https://public-xnmzdqumwy.now.sh/

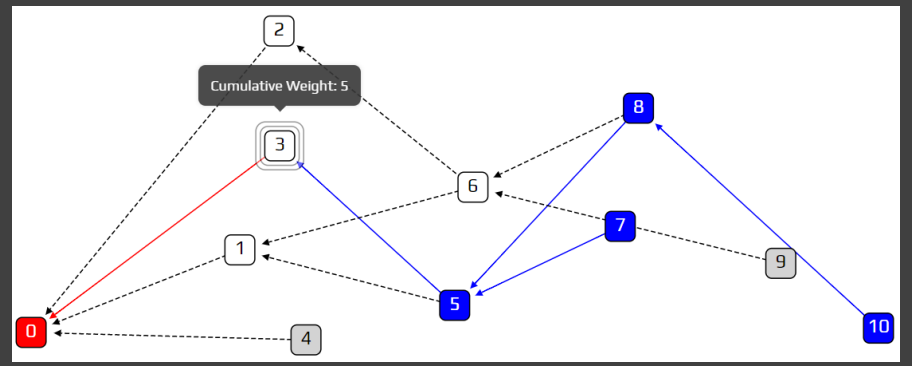
Issue: Lazy Tips

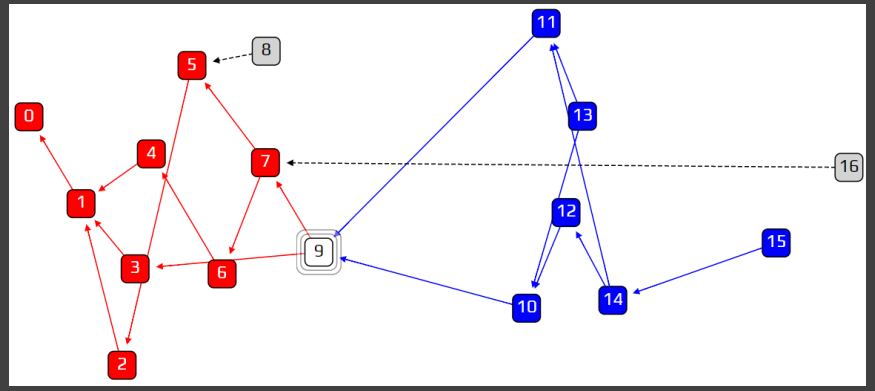


Tip Selection Algorithms

3. Weighted Random walk

Cumulative weight: denote importance of a transaction

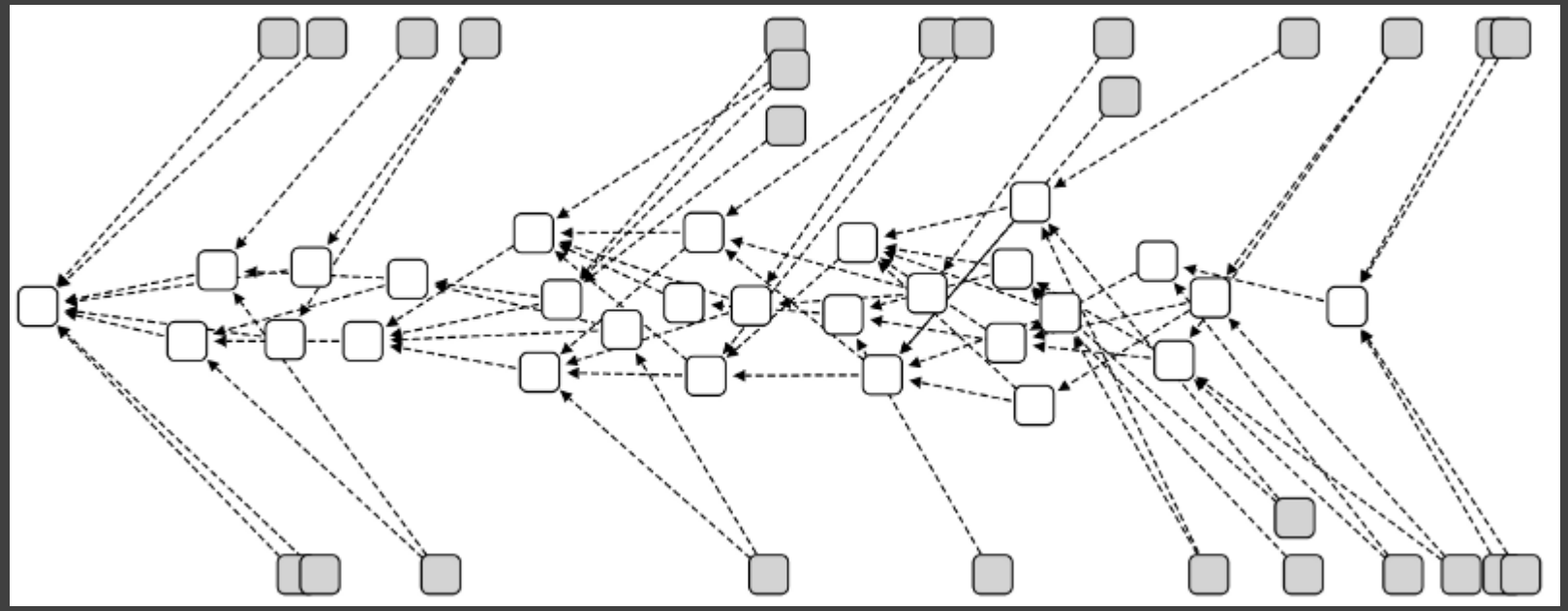




Tip Selection Algorithms

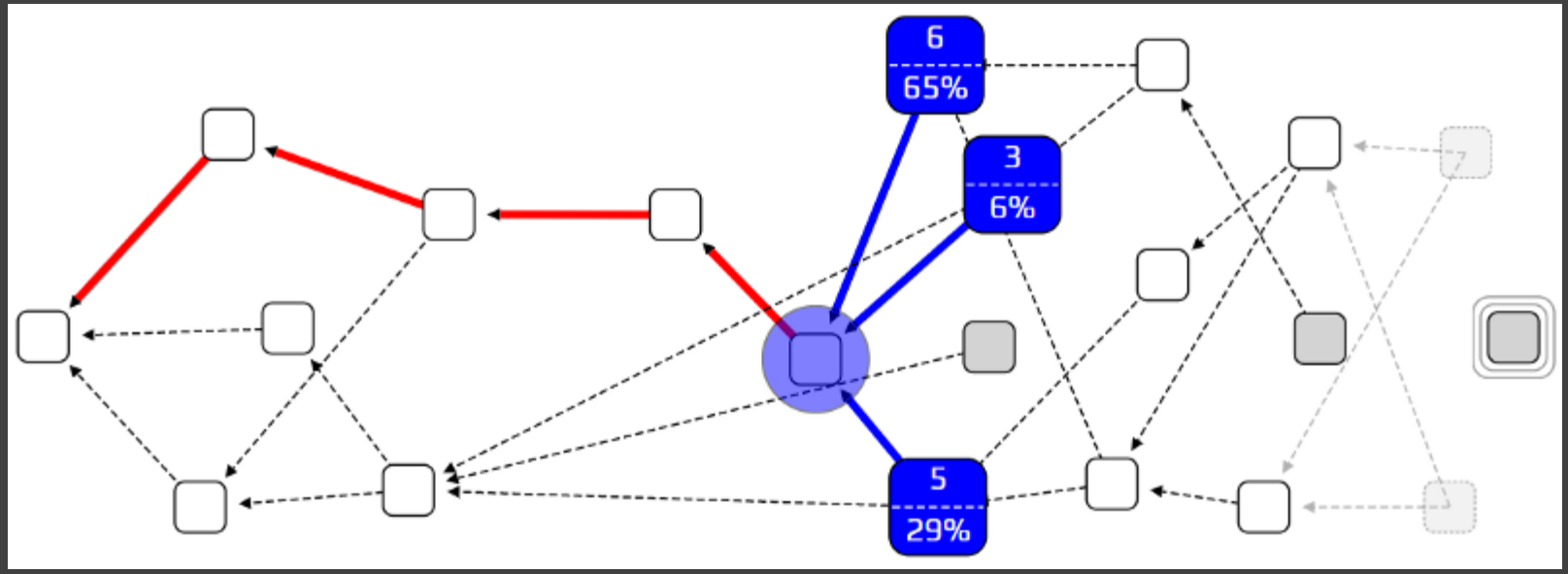
4. Super-weighted walk

Issue: forgotten tips on the sidelines



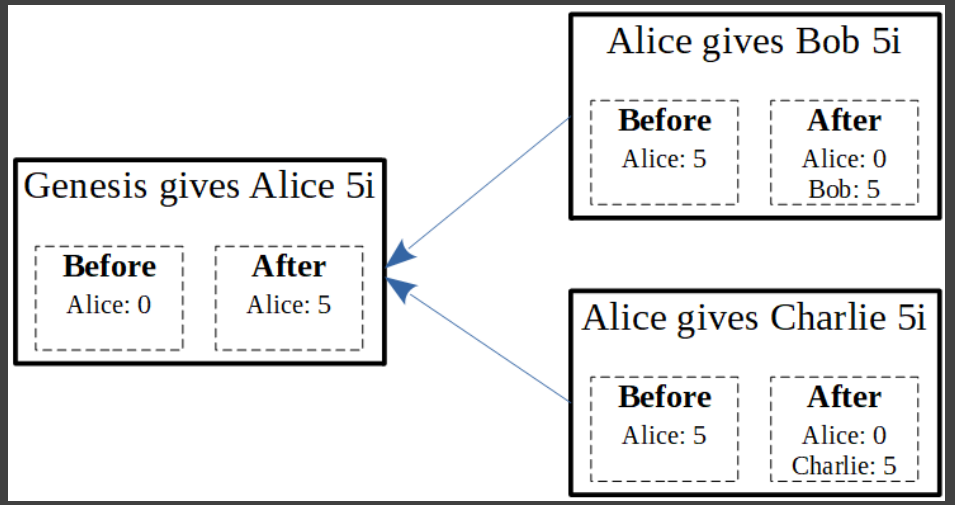
Tip Selection Algorithms

5. ***Markov Chain Monte Carlo*** technique, or MCMC



Double Spend & Confirmation Confidence

Solution to double spend: Weighted walk, one of the branches will grow heavier than the other, and the lighter one will be abandoned



Confirmation Confidence: Measure of a transaction's level of acceptance by the rest of the tangle

https://public-krwdbaytsx.now.sh/

Coordinator Nodes: Temporary different consensus mechanism for security reasons

IOTA

Meetup #2

Transactions in IOTA Tangle

Event Organizers

dcentrum Community

Connect | Collaborate | Create

Event Supporters

nagarro.

THINKING BREAKTHROUGHS

IOTA Transaction Bundles

A Transaction is a unit of multiple attributes like address. It may for depositing IOTAs or withdrawal of IOTAs or sending message

Transaction Attributes (2673 trytes)

- ❑ signatureMessageFragment
- ❑ Address
- ❑ value
- ❑ timestamp
- ❑ currentIndex
- ❑ lastIndex
- ❑ bundle
- ❑ trunkTransaction
- ❑ branchTransaction
- ❑ Nonce

Transaction Types

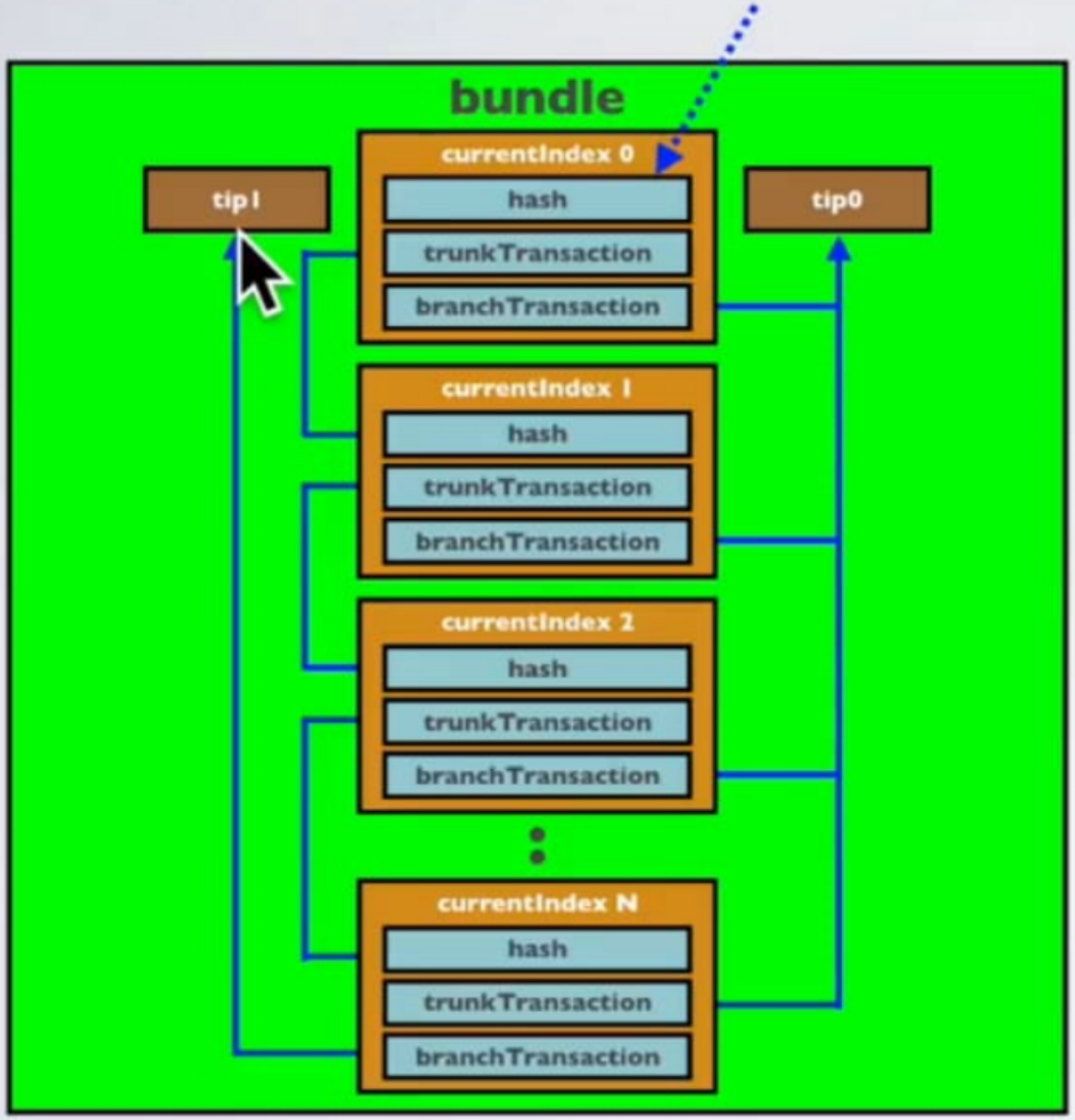
- ❑ Input transaction (withdraw)
- ❑ Output transaction (Deposit / message)
- ❑ Meta Transaction (for signature fragments)

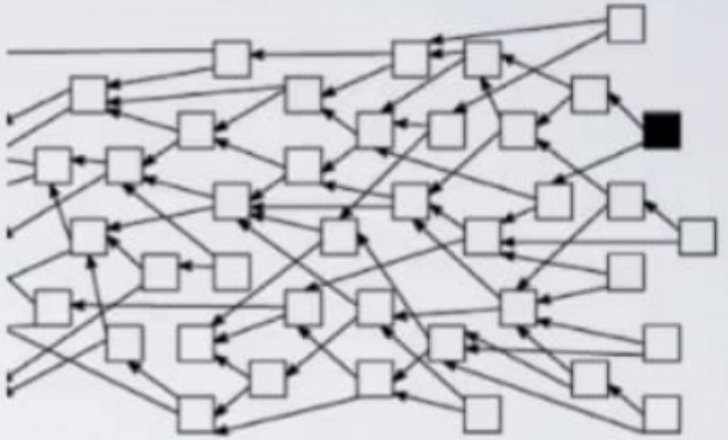
Transaction Bundle structure

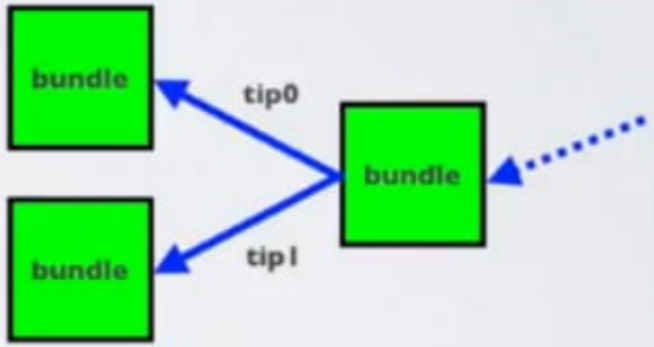
A bundle is an atomic unit of one or more transactions

index	Contents	Transaction type
0	Recipient's address, positive value and sign	output / Deposit
1	Sender's address and the first part of its signature Negative value	Input / withdrawal
2	Sender's address and the second part of its signature Negative or zero value	Input / withdrawal
3	Sender's address and the rest of its signature	Meta transaction
4	Sender's address and positive value	Output / deposit

TRANSACTIONS IN BUNDLE








```
currentIndex 0 = tail transaction
currentIndex N = head transaction
```

Prepare transactions

Prepare one or more transaction with senders or receivers addresses and values sign all input transaction with sender's keys using key generator

Output

Transaction

```
Address   : QQQQQQ......QQQ
Value     : 80
Tag       : VISUALTRANSAC
Timestamp: CurrentTime()

Index     : 0
LastIndex: 3
Bundle    :
Nonce     :

Message   : WELCOME9TO9IOTA
```

Input

Transaction

Transaction

```
Address   : AAAAAA......AAA
Value     : -100
Tag       : VISUALTRANSAC
Timestamp: CurrentTime()

Index     : 1
LastIndex: 3
Bundle    :
Nonce     :

Message   :
```

Remainder

Transaction

```
Address   : EEEEEE......EEE
Value     : 20
Tag       : VISUALTRANSAC
Timestamp: CurrentTime()

Index     : 3
LastIndex: 3
Bundle    :
Nonce     :

Message   :
```

Sign Transactions

Sign all input transactions with private key

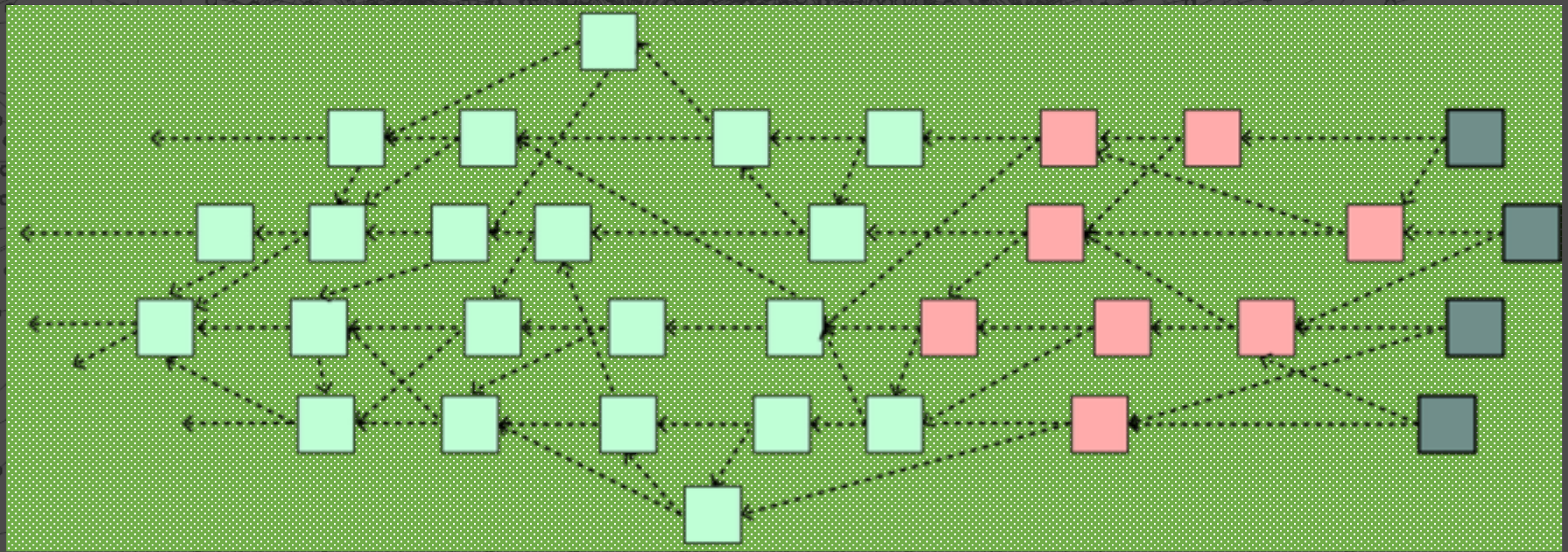
- Seed 81 trytes
- Private and Public Key
- Address
- Signature for input transactions
  - Hash based One time signature (Winternitz) using Signature Fragment Generator
  - Use Address only once to send IOTAs

Prepare bundle

1. Generate bundle hash.
2. Assign bundle hash to transactions

Tip Selection

1. Every transaction bundle should reference to two previous unconfirmed transaction as parent transaction
2. Process used MCMC algorithm to pickup these tip selections



Proof of work

1. Get trytes of transaction
2. Get minimum weight magnitude (this is 9 for test net and 14 for mainnet)
3. Execute pow function in with MWM and transaction tryets
4. The above step returns the nonce.
5. Include the nonce with transaction trytes
6. Execute curl hash with the new transaction tryes. This returns the transaction hash

7. If the this hash matching difficulty no of 9s at the end, then transaction is valid, otherwise repeat the same process by incrementing the nonce

```
pow( ttrytes, mwm ) = nonce,
trans_hash = ‘’
white trans_hash.endswith(‘9999’) == false
        trans_hash = curlhash( ttrytes+nonce )
```

1. Broadcast the bundle to the tangle

IoT hands on lab

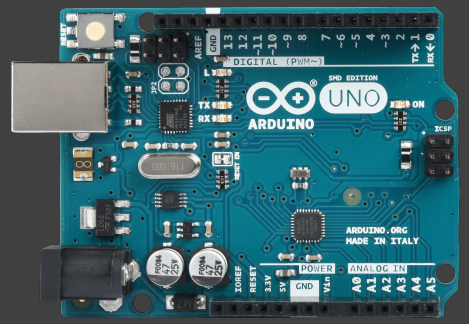

WHERE?
when?
which?
WHO?
why?
WHEN?
How?
WHERE?
WHAT?

Sensors

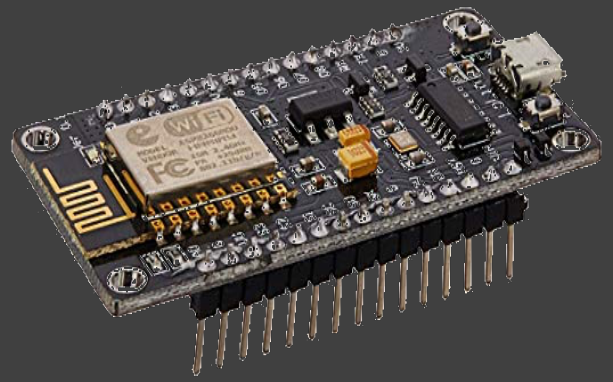
Automative	Healthcare	Manufacturing	Retail
Pressure Sensor	Vitals Sensors	Ultrasonic Sensors	NFC
Vibration Sensor	Occupancy Sensor	RFID	Motion sensor
Sound Decibel Sensor	Air Quality Sensor	Smoke Sensor	CO2 sensors
Motion Sensor	Luminosity Sensor	Camera	Camera
Angle Sensor	Smoke Sensor	Temperature	RFID
Visibility Sensors	RFID(Asset tracking)	IR sensors	Weight sensors

Devices

Raspberry PI



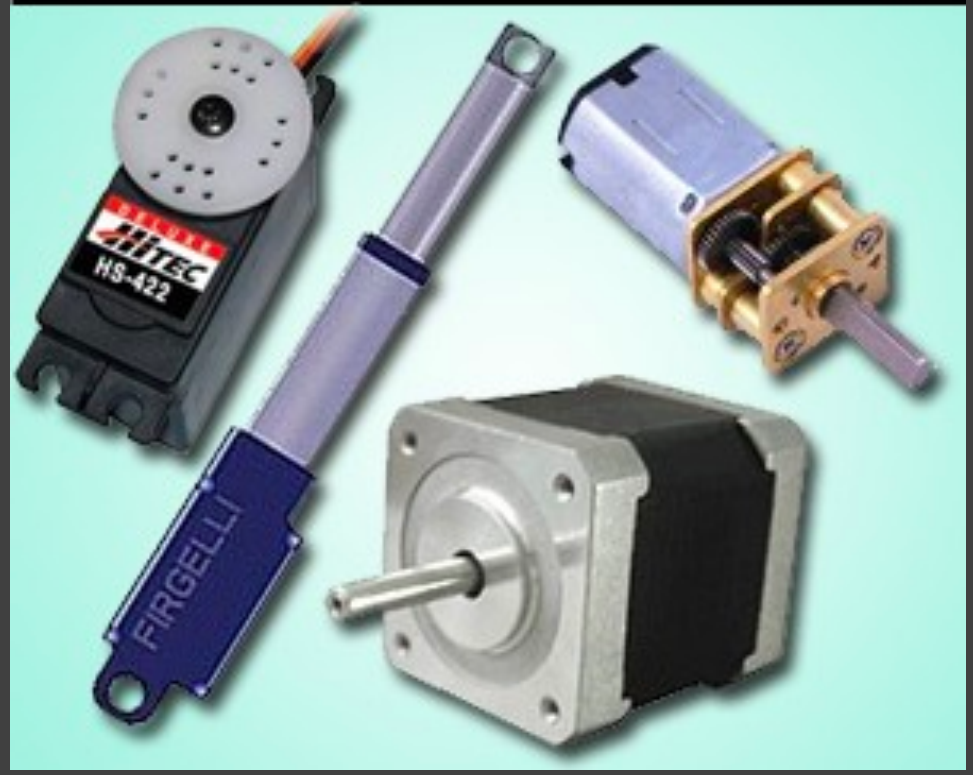
Arduino Uno



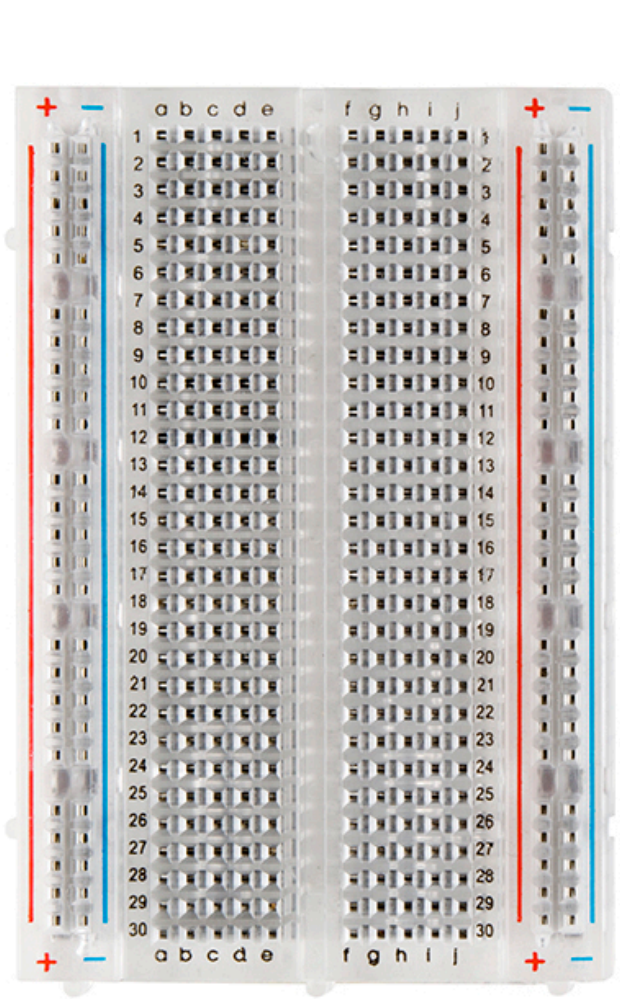
Node MCU

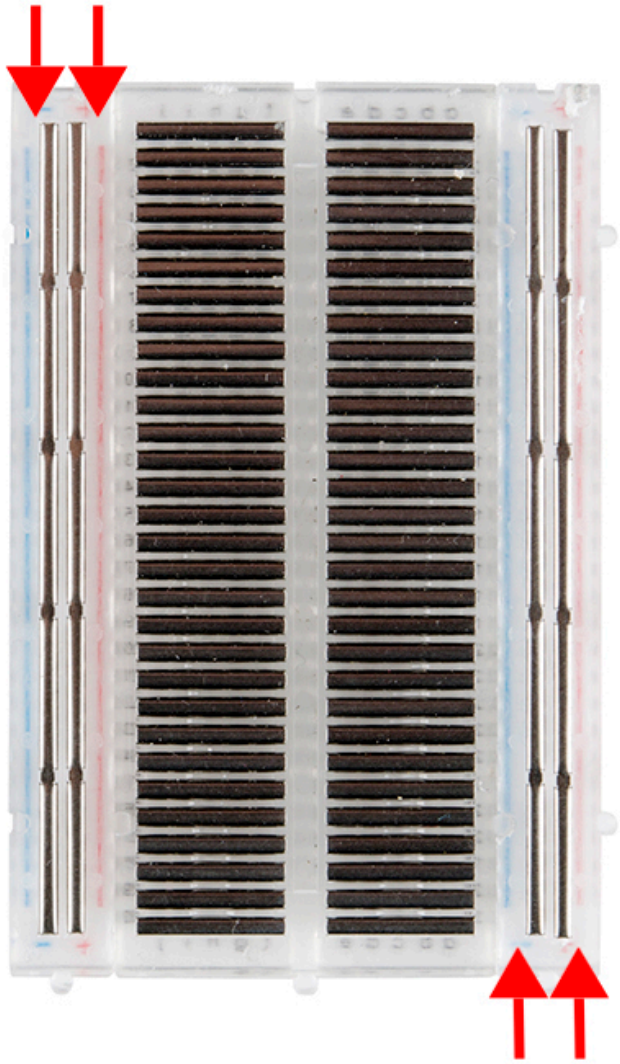
Intel Edison

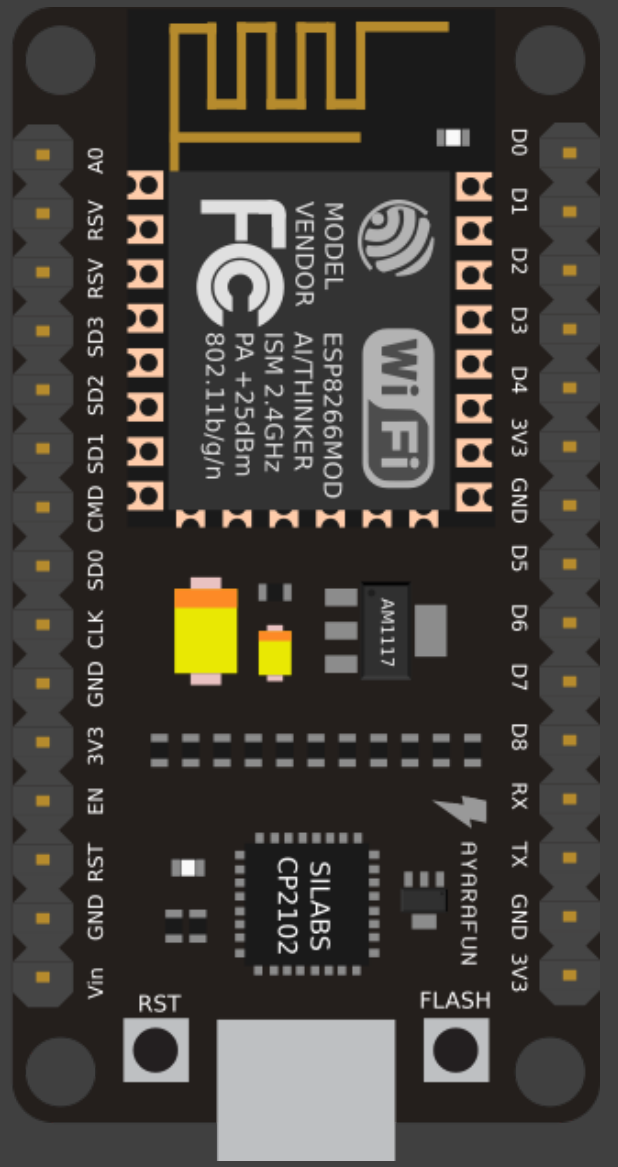
ACTUATORS



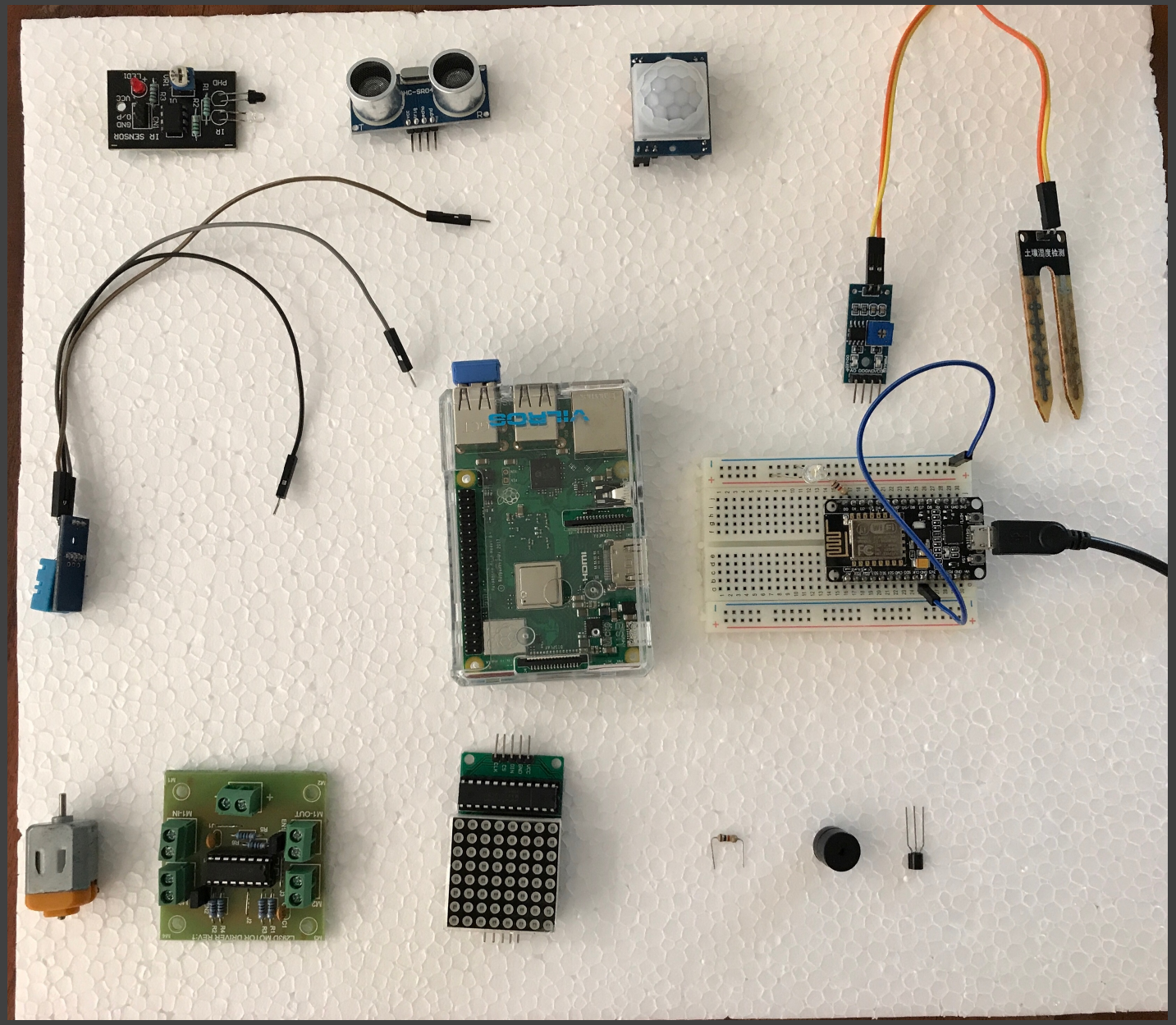
Breadboard Layout & Node MCU Pin Out Diagram







Some Hardware



Temperature Sensor, Node MCU, LED Actuator