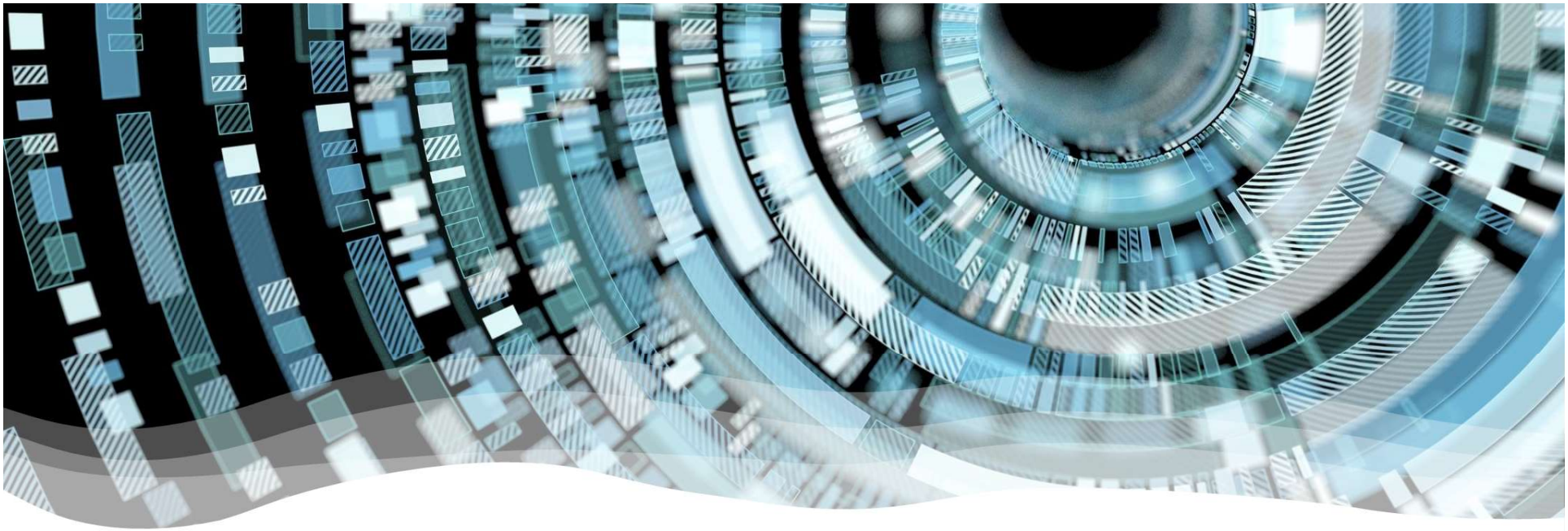
BLOCKCHAIN ASSOCIATION SINGAPORE

SP PACE ACADEMY SINGAPORE POLYTECHNIC SP

In support of SG JOBS & SKILLS



Enterprise Blockchain Developers (Intermediate)

Powered By

SmartMesh®

MeshBox

© 2017-2020 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.

Day 7 Lecture

SmartMesh and MeshBox Technology, In-Depth

How We Facilitate Inclusive Connectivity

18 January 2021

© 2017-2020 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.

Agenda

- HyperMesh Architecture : CyberPhysical IoT and Blockchain
- SmartMesh NFT for and MeshBox DeFi Model
- SmartMesh Spectrum Consensus
- Spectrum and Atmosphere Crosschain
- Photon Layer2 Off-Chain State-Channel for Spectrum

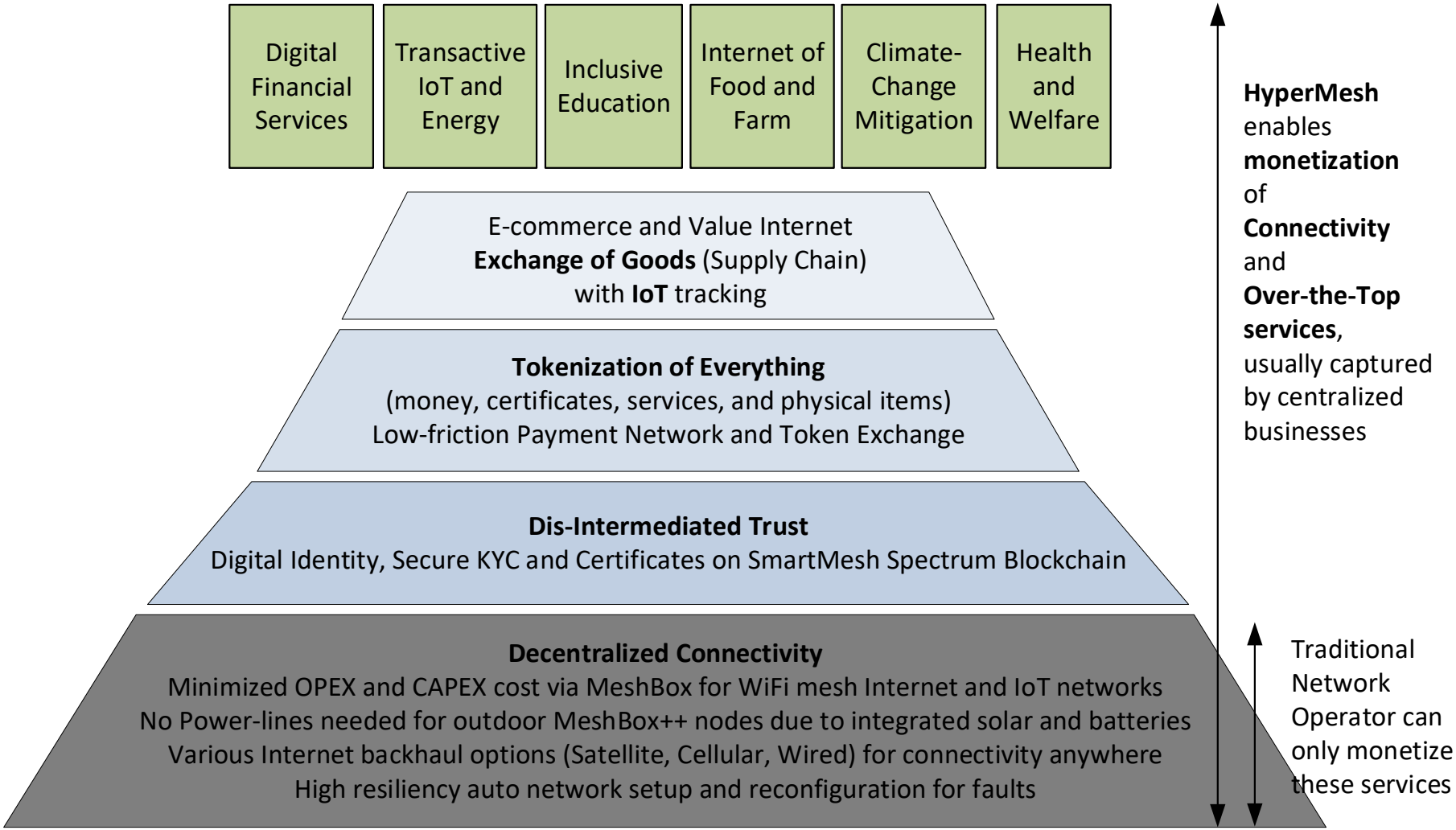
© 2017-2020 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.

HyperMesh Infrastructure

- History and evolution of Internet
- Innovation to infrastructure and architecture – solutions to achieve inclusiveness: Mesh Network
- What problems can SmartMesh and MeshBox solve?

© 2017-2020 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.

HyperMesh Over-the-Top Services Monetization

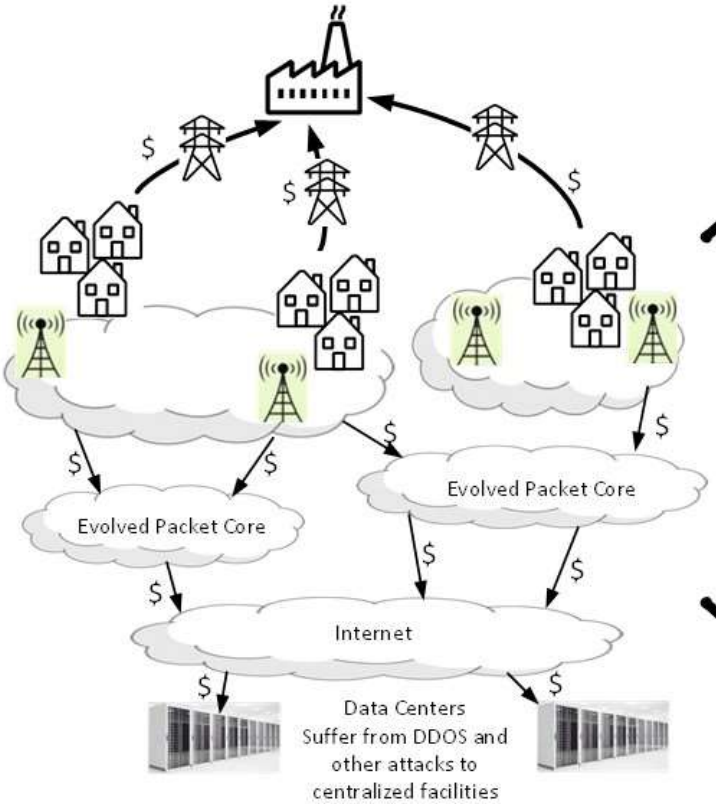


© 2017-2020 SmartMesh Foundation Pte. Ltd., MeshBox Foundation Pte. Ltd..

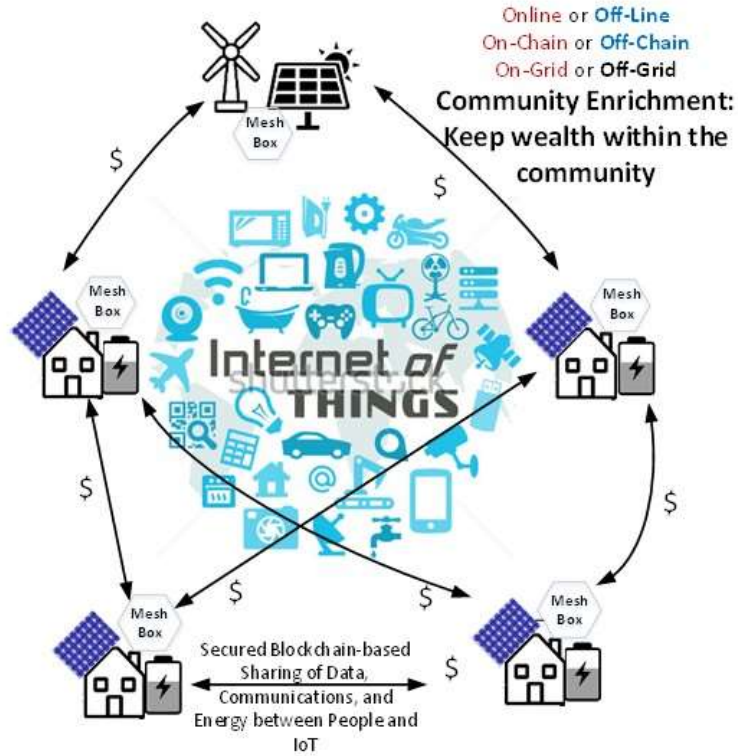
SmartMesh MeshBox

HyperMesh Infrastructure Evolution

Conventional Service Provider Model



Grassroots Service Provider Cooperative



Wealth Taken OUT of Community

Wealth Kept INSIDE of Community

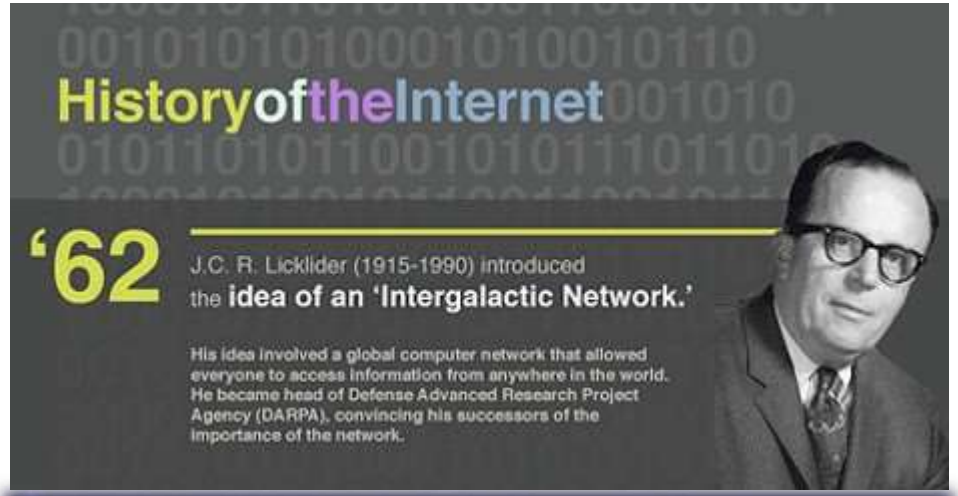
- Community members are not dependent on Operators, and can setup and run their own HyperMesh Infrastructure.
- Wealth is re-circulated within the community through Peer-to-Peer payments for Wifi, Content delivery, Banking, and E-Commerce.

SmartMesh MeshBox

© 2017-2020 SmartMesh Foundation Pte. Ltd., MeshBox Foundation Pte. Ltd..

History of the Internet

- 1962, MIT's J.C.R. Licklider popularized the idea of an "Intergalactic Network" of computers, which ultimately led to the creation of the ARPAnet. The founding father got his BA in Physics at Washington University in St. Louis.
- 1969，Leonard Kleinrock，Packet Switching，MIT----UCLA，First Internet Node
- 1983，Robert Kahn and Vinton Cerf developed TCP/IP which was adopted by ARPAnet.
- 1990, Tim Berners-Lee invented the World Wide Web.
- 2018, Internet founding fathers expressed concern about the Internet, which has become more and more centralized.



© 2017—2020 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.,

Current Infrastructure and Internet Failed at Inclusiveness

- March, 2018, the WWW turns 29 years old. Status:

  Berners-Lee, in an open letter to mark the 29th anniversary of his invention, said: "In recent years, we've seen conspiracy theories trend on social media platforms, fake Twitter and Facebook accounts stoke social tensions, external actors interfere in elections, and criminals steal troves of personal data."
  These problems have proliferated because of the concentration of power in the hands of a few platforms – including Facebook, Google, and Twitter – which "control which ideas and opinions are seen and shared".

- Digital divide : 4 Billion people are unconnected to the internet
- Financial Divide: 2 Billion people are without financial services
- Clean Energy Divide: 1 Billion people without electricity

- Is it because lack of Money? NO

Our centralized financial and control structure is to blame

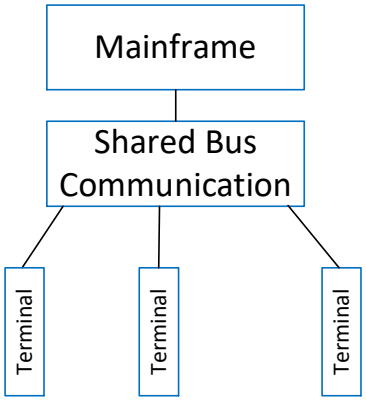
- https://www.theguardian.com/technology/2018/mar/11/tim-berners-lee-tech-companies-regulations

© 2017-2020 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.

Internet and Communications Evolution

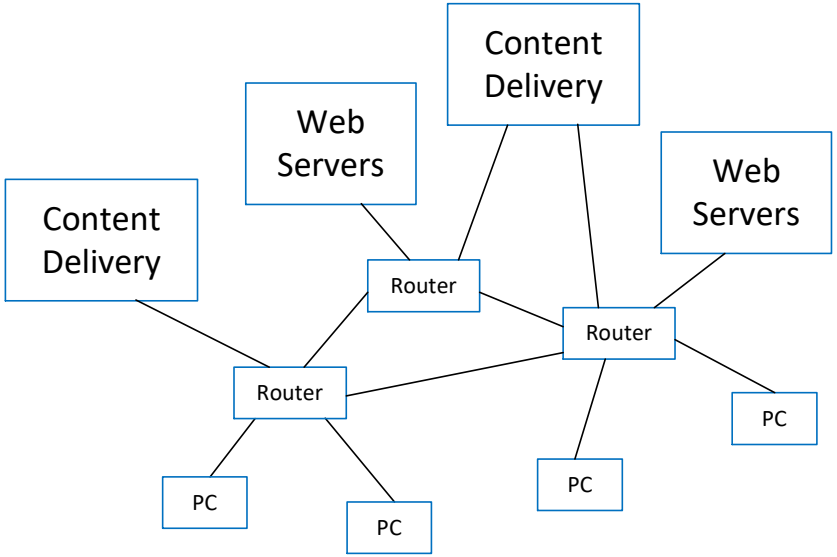
1. Mainframe Computers and Voice-Communications

Centralized
Circuit-Switched
Cellular 1G 1980s ; 2G 1990s



2. Internet : Personal-Computers, Data-Communications

Centralized
Cellular 3G 2000s
Circuit-Switched Voice
Packet-Switched Data



© 2017-2020 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.

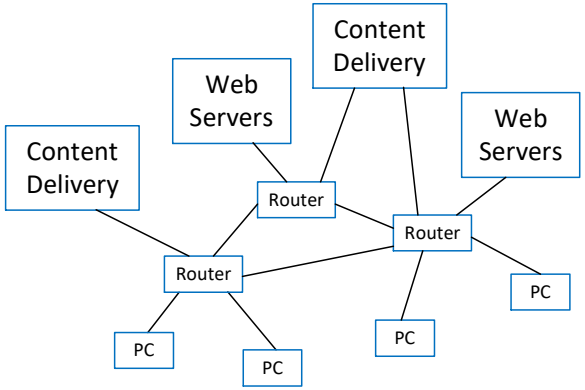
Internet and Communications Evolution

2. Internet : Personal-Computers, Data-Communications

Centralized

Cellular 3G 2000s

- Circuit-Switched Voice
- Packet-Switched Data

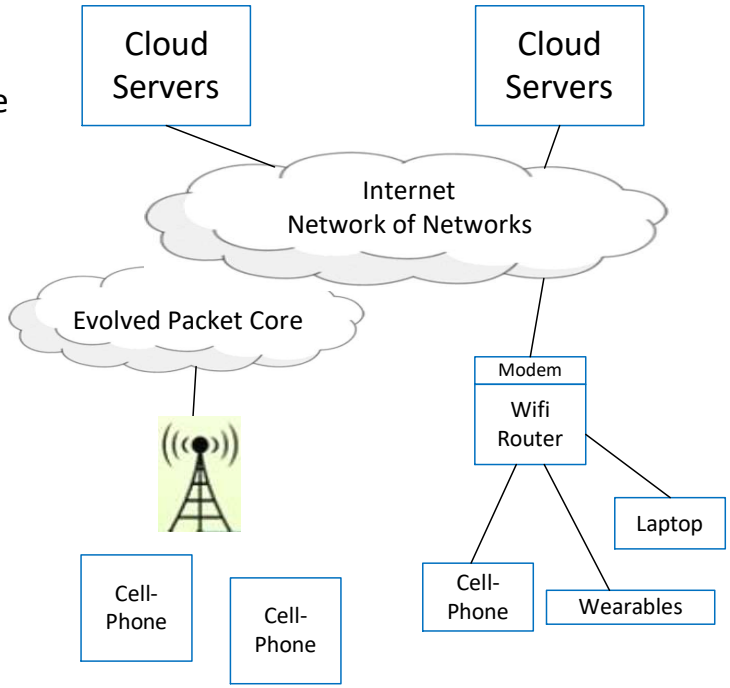


3. Cloud : Software defined Networking/Computing/Storage

De-Centralized

Cellular 4G 2010s

- Packet-Switched Voice
- Packet-Switched Data



© 2017-2020 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.

Internet and Communications Evolution

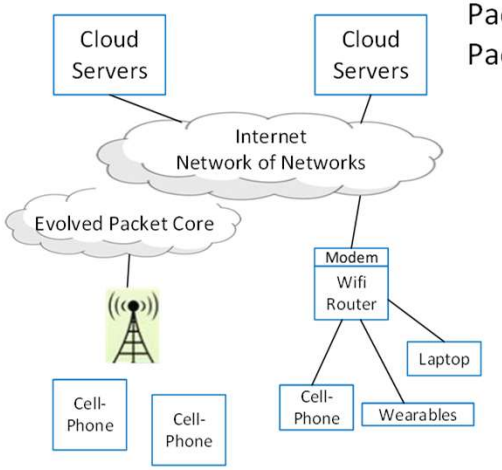
3. Cloud : Software defined Networking/Computing/Storage

De-Centralized

Cellular 4G 2010s

Packet-Switched Voice

Packet-Switched Data



4. Hyper-Mesh : Internet of Value with Mesh Networking

Distributed

Cellular 5G 2020s Interoperability

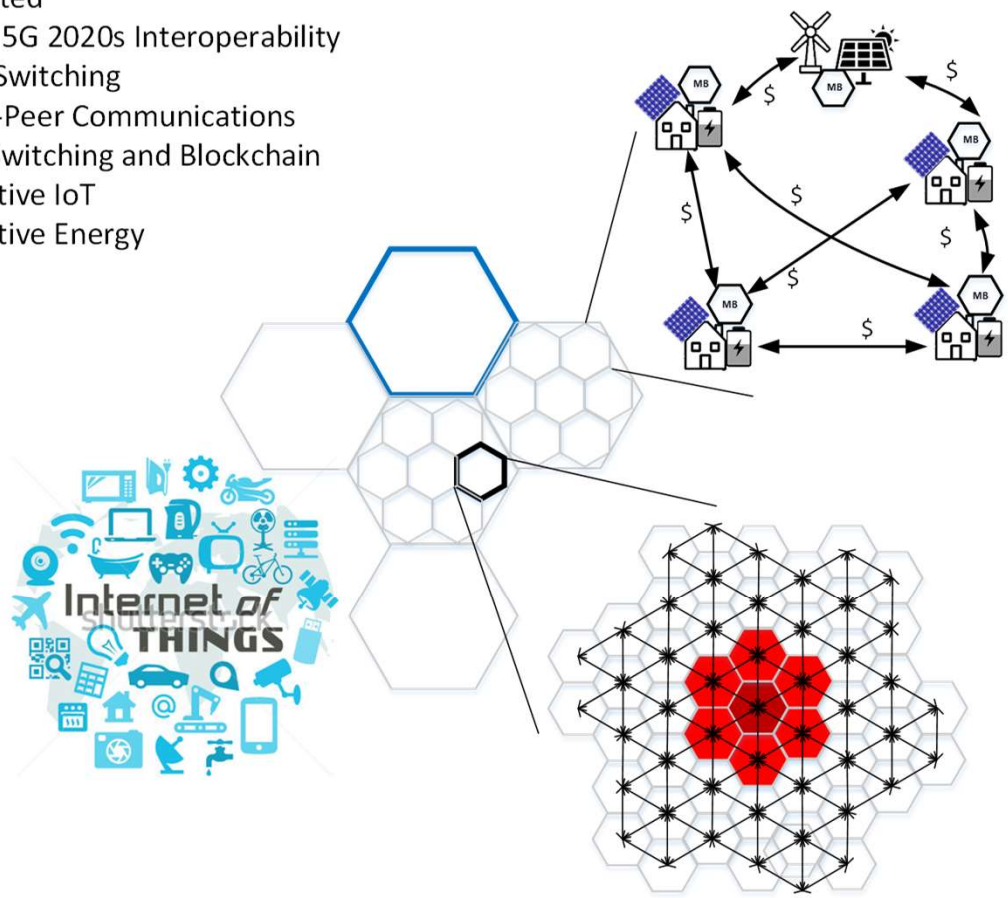
Packet-Switching

Peer-to-Peer Communications

Token-Switching and Blockchain

Transactive IoT

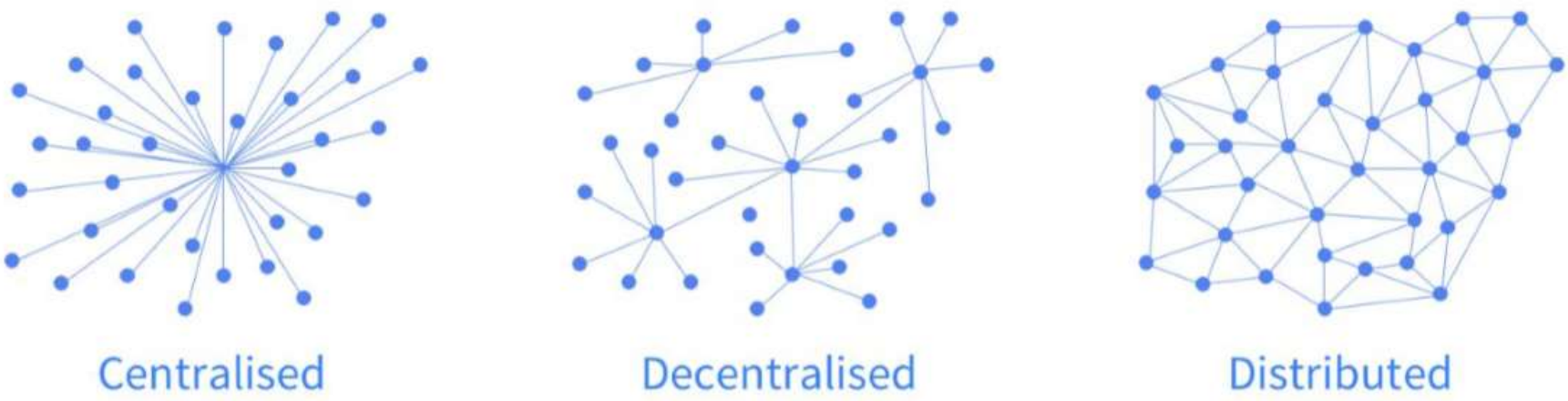
Transactive Energy



© 2017-2020 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.

Mesh Network

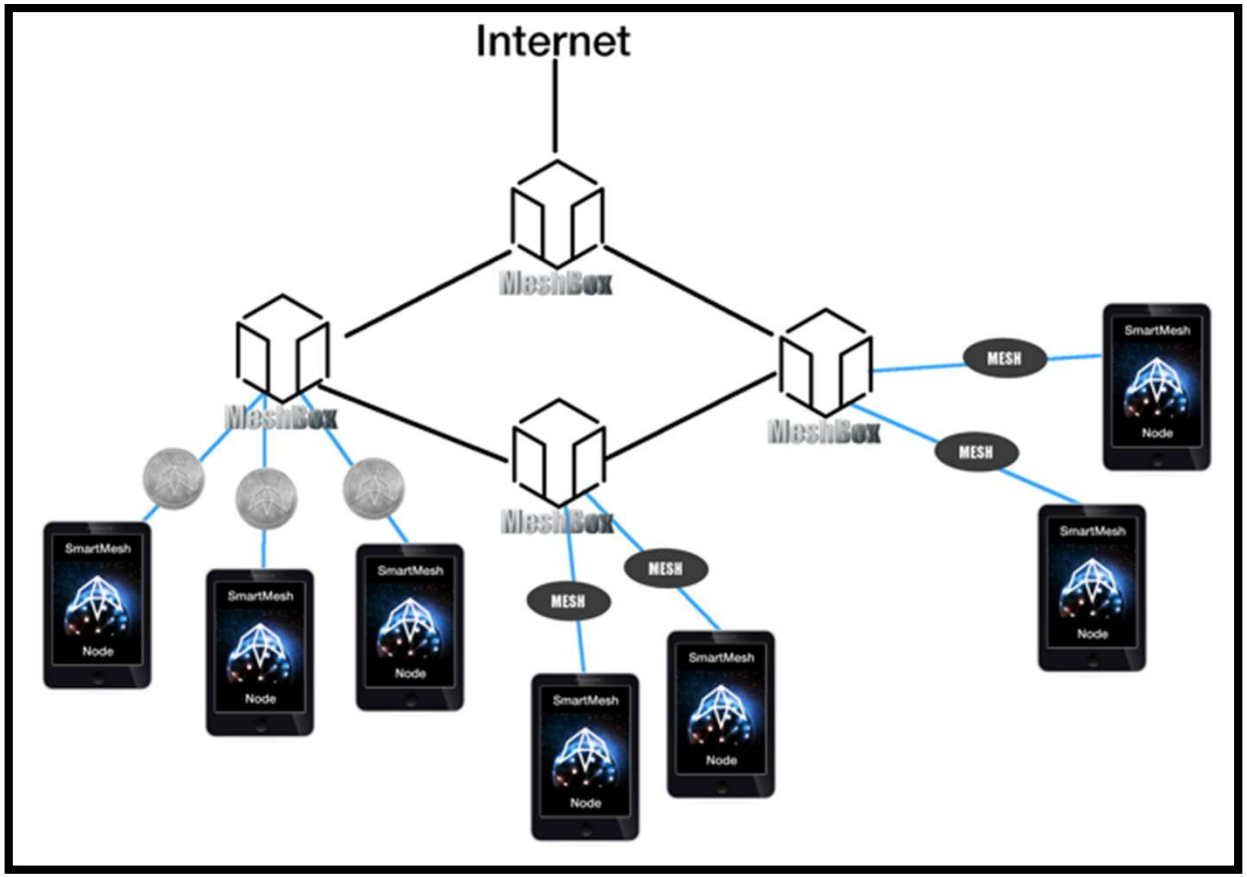
- Mesh advantages:
  - Easy to deploy and install
  - Wireless transmission
  - Robust network
  - No single point of failure, Flexible structure, High bandwidth.
- Mesh disadvantages:
  - Large-scale mesh networks requires relay nodes, which are difficult to incentivize…
  - Until the Blockchain



© 2017—2020 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.,

Meshbox Ecosystem Topography

- Gateway functionality
- Network hub for routing, storage and content distribution
- Atmosphere：Second Layer Cross Chain Interoperability
- Universal Payment Channel (Wormholes)



© 2017—2020 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.,

HyperMesh Indoor use cases

- Company Security
- P2P Banking
- Control Center for Iot devices
- Transactive Energy control
- Dense user gatherings

- Homes & office buildings
- Hotels, Museums, Event Venues
- Shopping malls, Airports

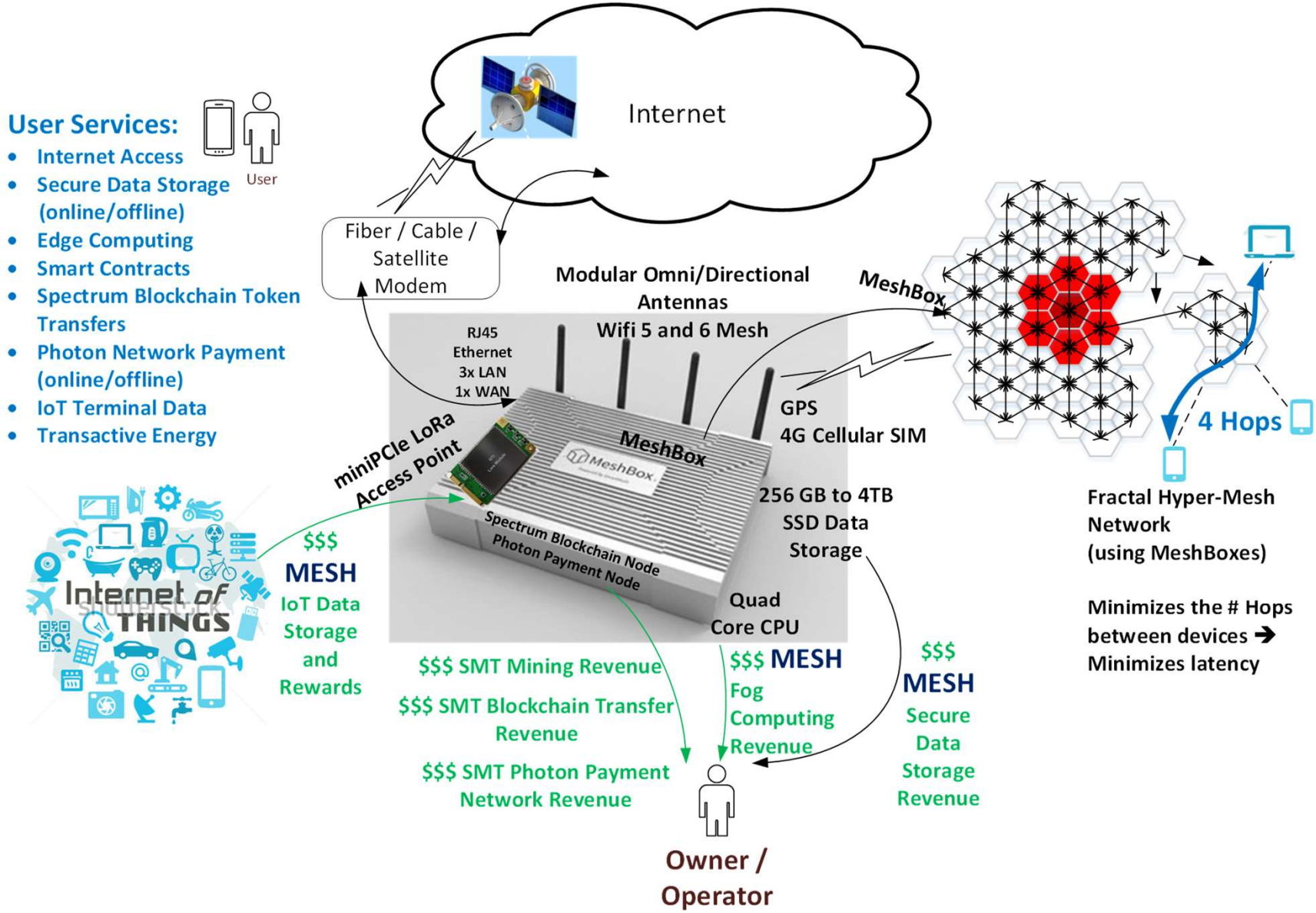
© 2017-2020 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.

Indoor : MeshBox

MeshBox-Maxwell	MeshBox-Tesla
Quad Core 1.6 GHz CPU	Quad Core 1.6 GHz CPU
256 GB SSD ; External Disk to 8 TB	256 GB to 4 TB Modular SSD
Internal Omni-directional Antennas for Wifi	Modular Omni/Directional Antennas for Wifi 5
Ethernet	Ethernet, LTE Backhaul, GPS, Integrated LoRa Access Point (Beijing GTI)

© 2017-2020 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.

MeshBox Features



© 2017-2020 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.

HyperMesh Outdoor Use Cases

- Adhoc Mobile Networks
- Internet gateway
- Disaster Stabilization

- Areas without infrastructure
- Dense populations
- Remote Areas, Farms, Fishing ports
- Festivals & Markets

NETWORK DEPLOYMENTS IN THE USA:

- Superbowl 51 February 2017 in Minneapolis, Minnesota : 6 MeshBox++ nodes
- 50th Special Olympics July 2018 in Chicago, Illinois : `15 MeshBox++ nodes, 3 gateways.
- Permanent installations of MeshBox++ networks in San Jose, and San Francisco, California

© 2017-2020 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.

Outdoor : MeshBox++ & GTI IoT Gateway

F865

4x4 Rugged Battery Node

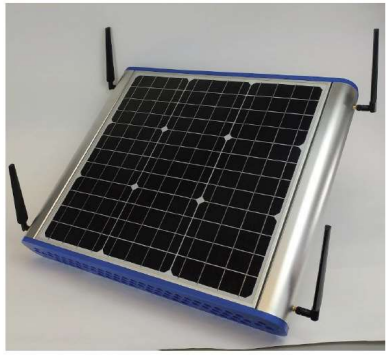
Dual-core 1.7GHz processor

4G-LTE-a backhaul

Optional 1TB SSD

IP68 Waterproof

S865



4x4 Solar-powered node

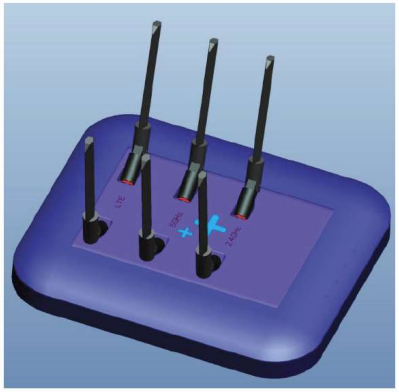
Dual-core 1.7GHz processor

4G-LTE-a backhaul

Optional 1TB SSD

IP67 Waterproof

F428



2x2 Battery-powered node

Mass-production capable

Quad-core 700MHz processor

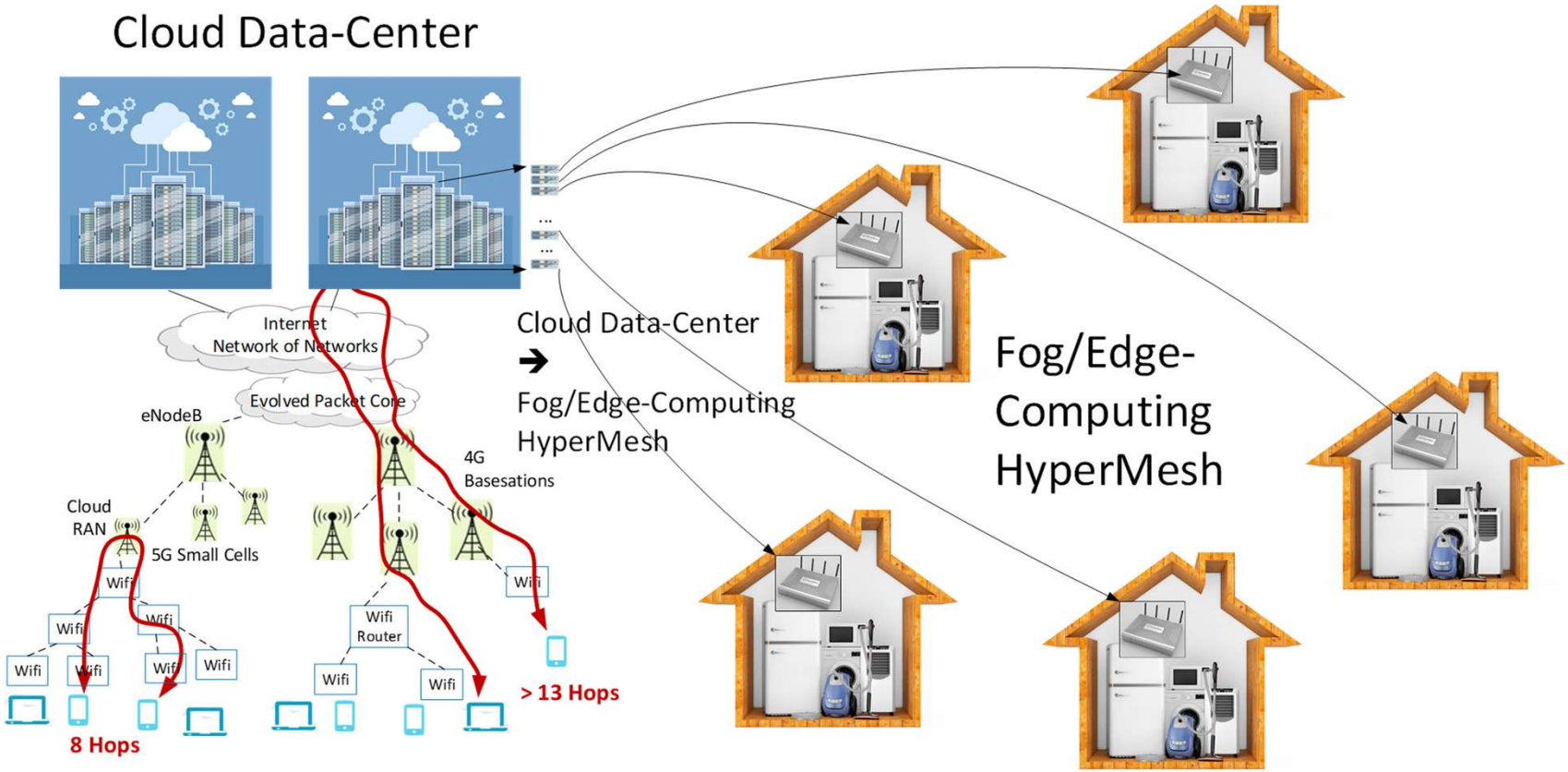
4G-LTE-a backhaul

Water-resistant

- Beijing GTI IoT Technology
- AP-5158 LoRaWAN Gateway
- 8-Channel LoRa Standard
- 400 to 915 MHz
- 25 km omni-directional range

© 2017-2020 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd. | Meshplusplus Inc.

HyperMesh Edge/Fog Computing/Storage



Users pay MeshBox owners in **MESH** tokens
to access decentralized Computing and Data Storage Services

- Research Reports Inc. Added New Report On Fog Computing Market. The Fog Computing market size, in terms of value, is expected to grow from USD 22.28 Million in 2018 to USD 203 Million by 2025, at a CAGR of +55% between 2018 and 2025. [RRI]
- Green Data Center market size to Exceed $ 174 B by 2024 +23% CAGR). [BW]

© 2017-2020 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.

HyperMesh Smart Ports

Photon Payment of MESH
Can carry IoT Data
➔ Higher efficiency

MeshBox with blockchain, compute and storage.

Outdoor MeshBox++
Battery and Solar IP68 and IP67

Indoor
MeshBoxes
Wifi Routers

LoRaWAN Access Point
Connecting a wide variety of IoT devices and Solar Panels

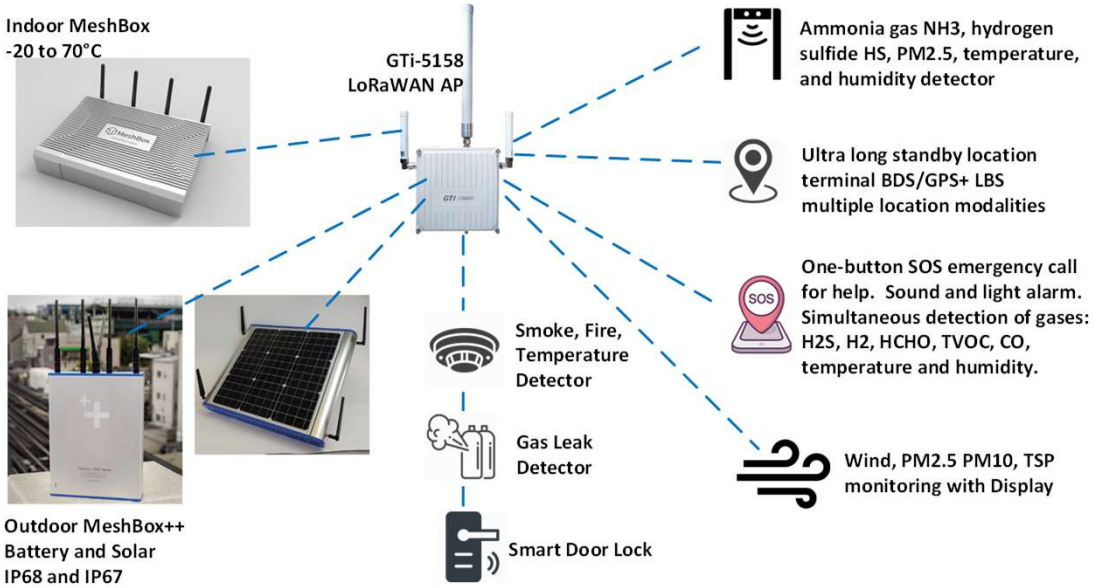
Wind, PM2.5
PM10, TSP
monitoring

Smoke, Fire,
Temperature
Detector

Solar Arrays

© 2017-2020 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.

HyperMesh Application at Airport

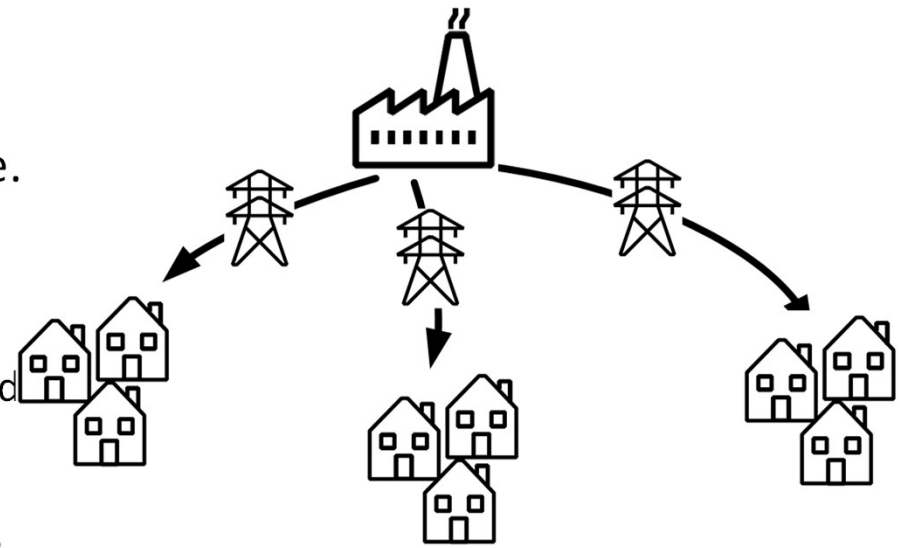


- Exploring collaboration with Nanyang Technological University in responding to Singapore Govt Grants
- Transactive Energy
  - 2x Energy generation per footprint with 3D Solar
  - Glare reduction techniques
- Meshed Communications
  - Decentralized
  - Low-latency P2P
- Realtime Control, Billing
  - IoT network monitors machinery, baggage transport system
  - Preventative maintenance
  - Photon transfers IoT data and **MESH** Payments simultaneously

© 2017-2020 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.

Traditional Electric Power System (EPS)

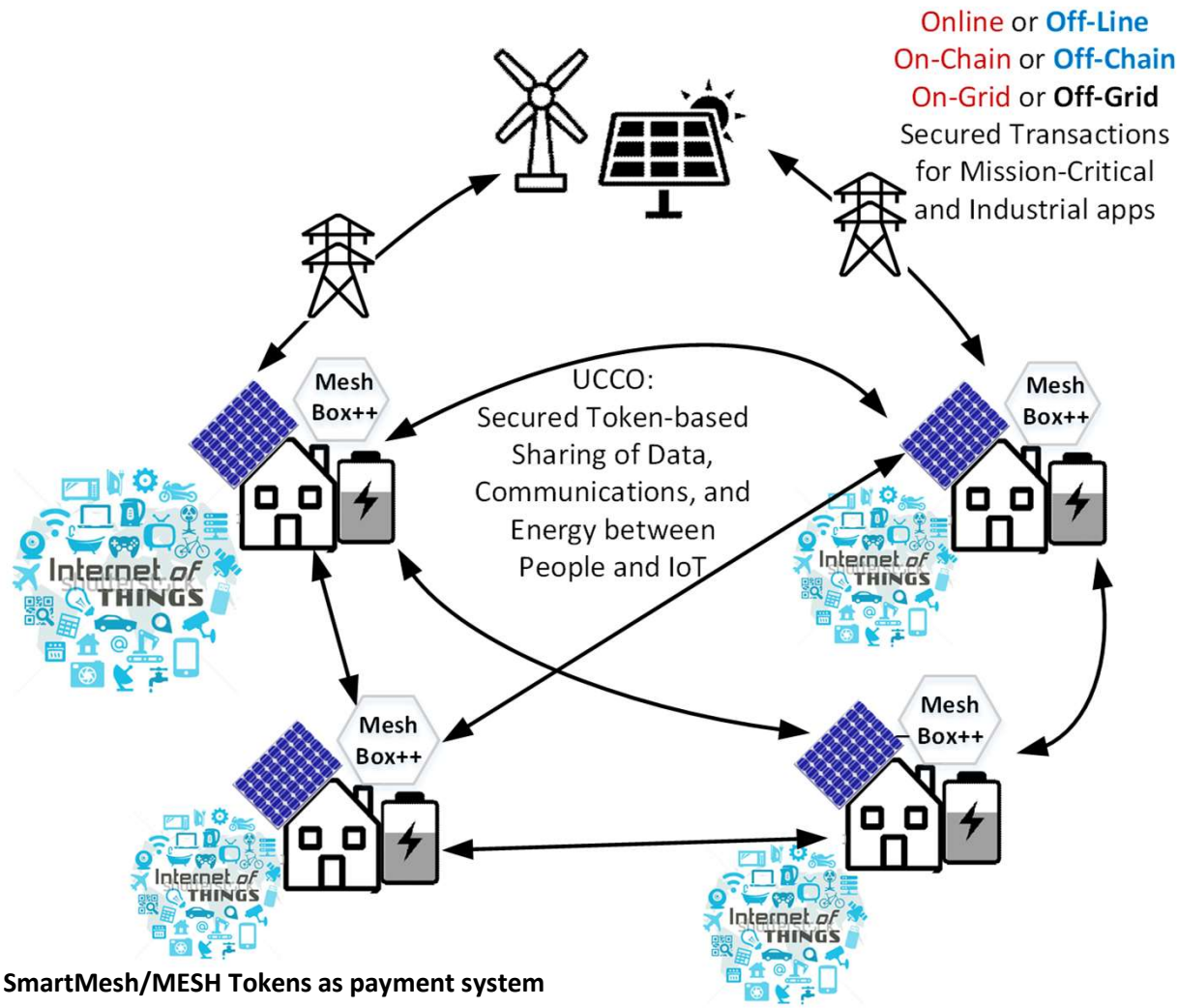
- Traditional EPS is composed of centralized Utility Plants (coal, gas, nuclear) and a transmission and distribution network to the end customers.
- Designed for the peak energy needed and is thus over-engineered for the worst-case.
  - Energy transmission is one-way and is delivered just-in-time with no storage of energy along the path (no buffering) from utility to consumers.
  - Just-in-time system: All the energy produced must match the energy consumed, on microsecond timescales.
- EPS is an Ultra-Large-Scale Cyper-Physical, tightly-coupled machine such that small faults in frequency and voltage can easily occur, causing the entire system to crash, leading to black-outs.



© 2017-2020 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.

TransActive-Energy and IoT

- Proliferation of Distributed Energy Resources (DER) such as solar, batteries, and wind due to an exponential cost reduction
  - While cost of traditional energy sources continues to rise.
  - Rooftop solar becoming cheaper than the transmission of electricity from Centralized Utilities [Seba].
- Peer-to-peer exchange of Energy between Prosumers (Consumers + Producers).
- HyperMesh enables people to act as Carriers, Utilities, and Media centers



Transactive Energy Electric Power System

Distributed, Peer-to-Peer Energy Auction with SmartMesh/MESH Tokens as payment system

(1) Electric Power System ➔ Transactive Energy

(2) Communications Network ➔ MeshBox, MeshBox++, Satellites

(3) Realtime Control and Finance ➔ Blockchain and SmartContracts

© 2017-2020 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.

DeFi Business Models and Applications

© 2017-2020 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.

MeshBox MBOX NFT Swap

MeshBox MBOX NFT Owner

(1)
After passing KYC, a participant transfers 2000 USDT to an Wallet owned by SmartMesh in order to swap for an MBOX NFT.

SmartMesh®

(2)
A MeshBox-Tesla is TOKENIZED as an MBOX NFT

MBOX NFT

Tango DAPP

MBOX NFT Owner

(3)
MBOX NFT is linked to the Owner's Private Key, managed by SmartMesh Tango DAPP.

(4)
MeshBox hardware is manufactured using the 2000 USDT

Note that persons and entities in <u>USA, China, and Singapore,</u> are NOT eligible to participate in the MBOX NFT swap, and subsequently the MeshBox Yield farming process. Interested participants will undergo a KYC process to enforce such eligibility.

MeshBox®

MeshBox Local Operator (MLO)

MLO

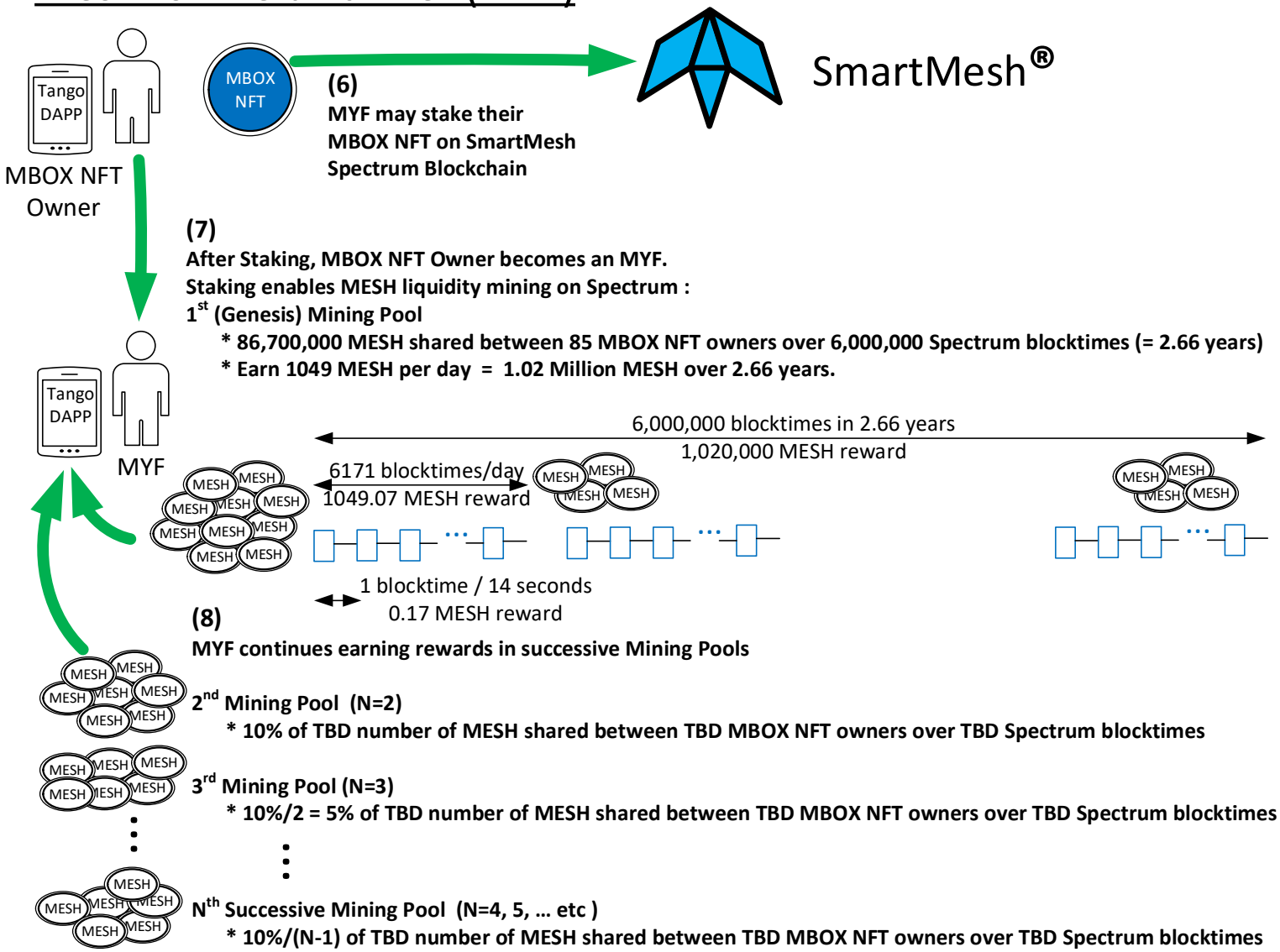
(5)
MeshBox hardware is transferred to the appropriate MLO in an underserved area.

SmartMesh MeshBox

© 2017-2020 SmartMesh Foundation Pte. Ltd., MeshBox Foundation Pte. Ltd..

MBOX NFT Staking for DeFi Yield Farming

MeshBox Yield Farmer (MYF)



(6)
MYF may stake their MBOX NFT on SmartMesh Spectrum Blockchain

(7)
After Staking, MBOX NFT Owner becomes an MYF.
Staking enables MESH liquidity mining on Spectrum :
1st (Genesis) Mining Pool
- *** 86,700,000 MESH shared between 85 MBOX NFT owners over 6,000,000 Spectrum blocktimes (= 2.66 years)**
- *** Earn 1049 MESH per day = 1.02 Million MESH over 2.66 years.**

(8)
MYF continues earning rewards in successive Mining Pools

2nd Mining Pool (N=2)
- *** 10% of TBD number of MESH shared between TBD MBOX NFT owners over TBD Spectrum blocktimes**

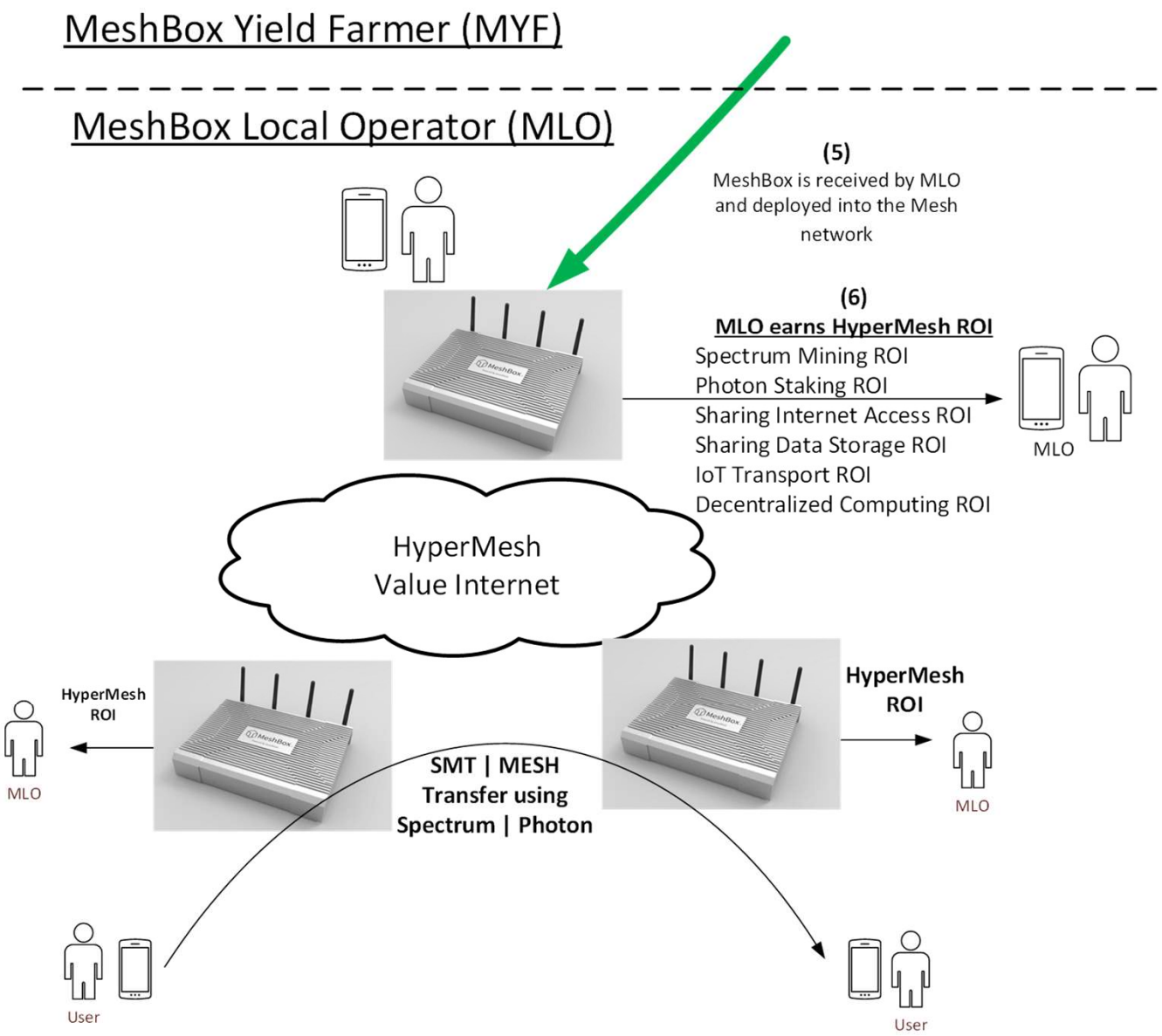
3rd Mining Pool (N=3)
- *** 10%/2 = 5% of TBD number of MESH shared between TBD MBOX NFT owners over TBD Spectrum blocktimes**

Nth Successive Mining Pool (N=4, 5, … etc)
- *** 10%/(N-1) of TBD number of MESH shared between TBD MBOX NFT owners over TBD Spectrum blocktimes**

© 2017-2020 SmartMesh Foundation Pte. Ltd., MeshBox Foundation Pte. Ltd..

SmartMesh MeshBox

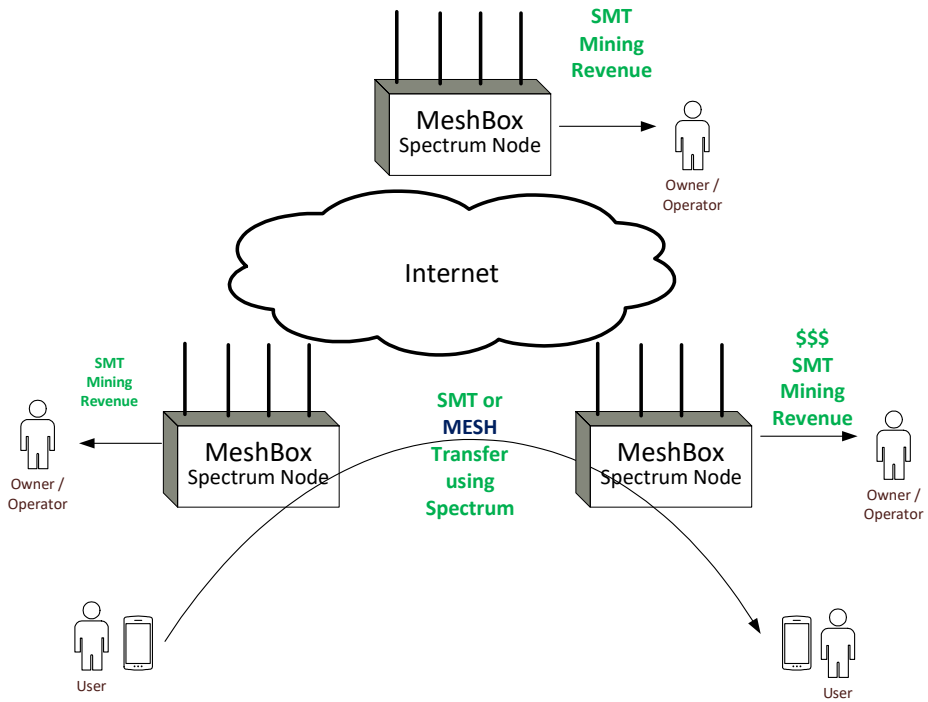
MeshBox Local Operator ROI



© 2017-2020 SmartMesh Foundation Pte. Ltd., MeshBox Foundation Pte. Ltd..

SmartMesh MeshBox

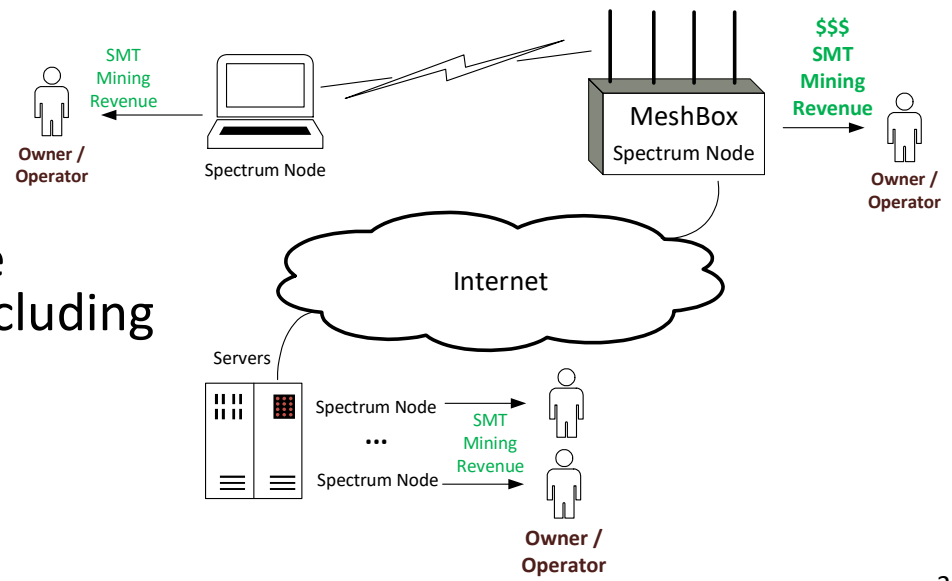
Spectrum Blockchain Mining ROI



Inclusive Payment System

MeshBox Owners/Operators earn SmartMesh Tokens (**SMT**) and **MESH** Tokens for staking SMT and running a Spectrum Mining Node

Tokens can be converted to Fiat Currency (SGD)



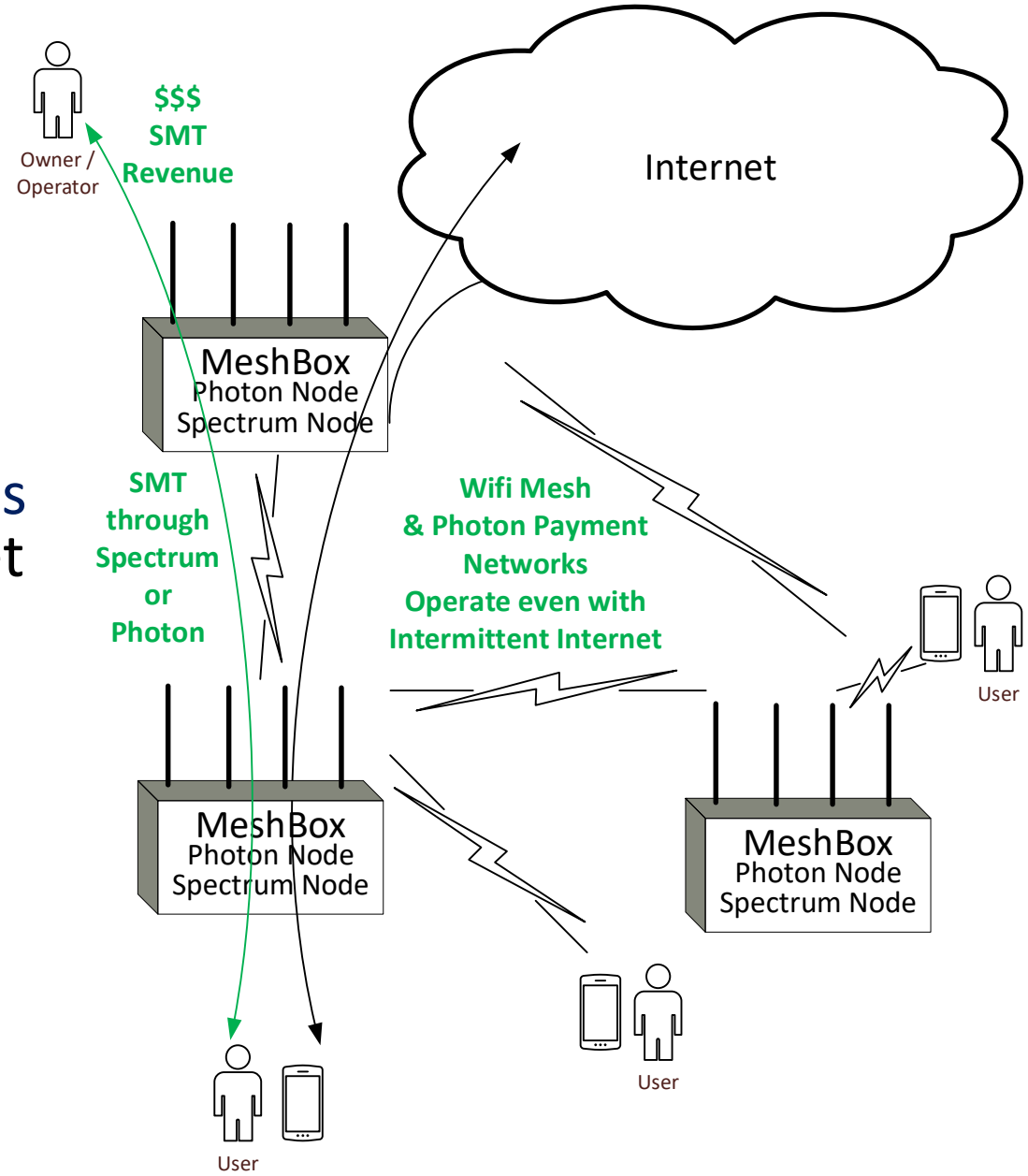
700 Spectrum Mining Nodes are currently running worldwide, including

- MeshBox
- Laptops
- Servers

© 2017-2020 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.

Sharing Internet Backhaul ROI

Inclusive Connectivity
MeshBox owners/operators earn SMT or MESH tokens by sharing excess Internet bandwidth with Mesh network.



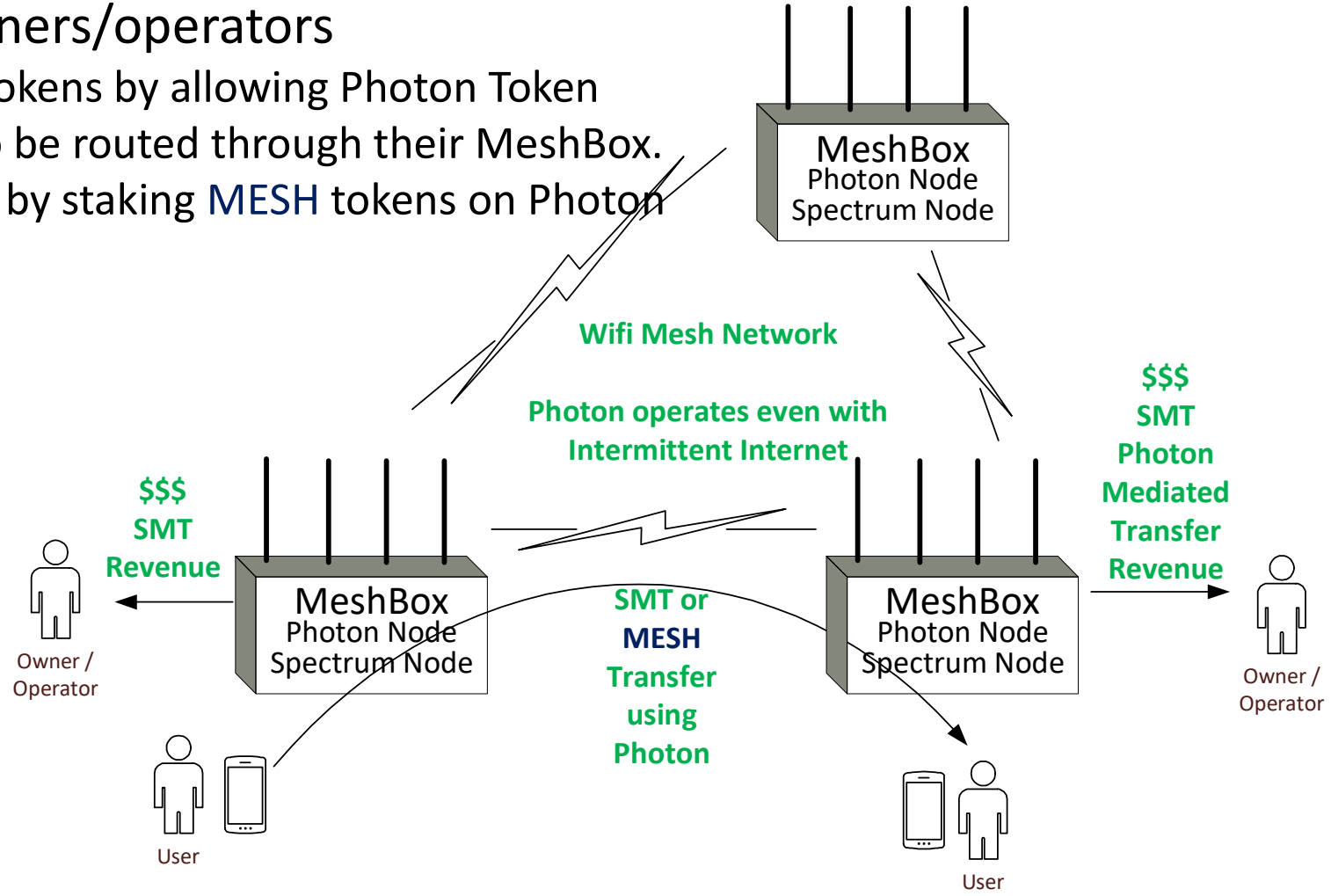
© 2017-2020 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.

Photon Payment Network ROI

Inclusive Payment System
Inclusive E-Commerce

MeshBox owners/operators

- Earn SMT tokens by allowing Photon Token transfers to be routed through their MeshBox.
- Earn MESH by staking MESH tokens on Photon Channels



© 2017-2020 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.

Sharing Disk Space

Inclusive Identity

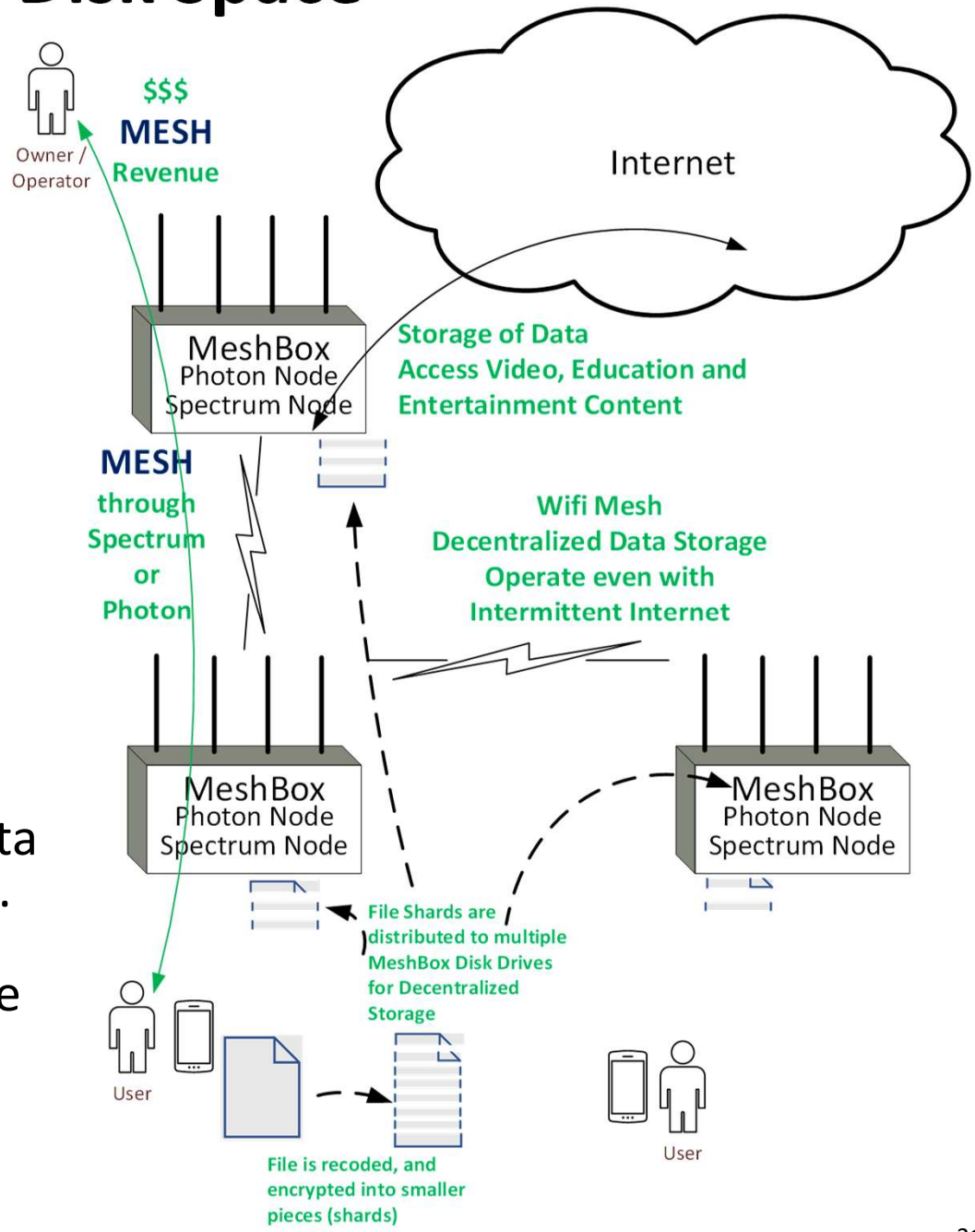
Inclusive Secure Data Storage

Inclusive Education

Transparency of Charity Donations

MeshBox owners/operators earn **MESH** by sharing Disk Space and providing Secure Decentralized Data Storage to users on Mesh network.

Integration with Tahoe-LAFS Secure Decentralized Data Storage

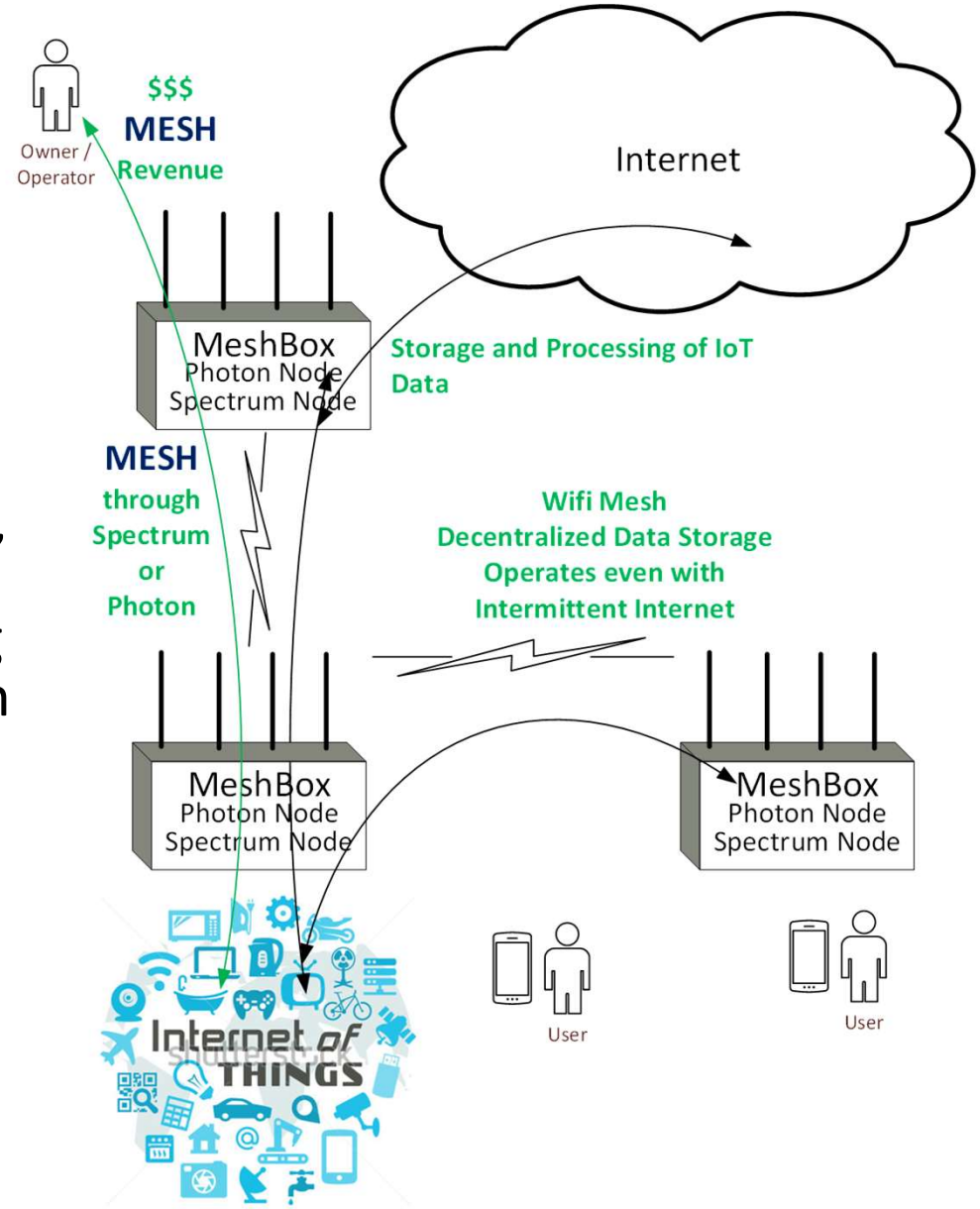


© 2017-2020 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.

Incentivized IoT Transactions

Inclusive IoT

MeshBox owners/operators earn **MESH** by sharing IoT Data, which is stored on MeshBox Edge Computing and Edge Storage Platform



© 2017-2020 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.

Spectrum Differentiation

- Low-Power, Well-suited for embedded IoT Applications
- Low Operational Expenses (Op-Ex)
  - Low-power costs for mining
  - Low Transaction Fees
- Two-Layer Security

The Need for Spectrum

- Why not use Ethereum ?
  - The blockchain data of Ethereum is too large, and cannot be supported on low-end embedded and Internet of things devices
  - Power costs for Ethereum Mining is too high
  - Ethereum transactions fees are high relative to poverty level standard of living
- SmartMesh developed Spectrum, as a public chain, compatible with Ethereum
  - Ethereum mints (generates) new tokens as a reward to the (Ethereum) node which wins the PoW competition (Finding a Golden nonce). The total number of Ethers in circulation can grow idefinitely
  - The total number of SMT has been pre-determined to be Pi Billion (3,141,592,654), all of which were created at the time of the ICO. The mining reward is transferred from SmartMesh to each successful Signing node.
- SmartMesh developed a secondary layer — Photon network
  - Photon minimizes the disk space for the Spectrum blockchain by offloading trivial Spectrum transactions.
  - Photon was brought online before Spectrum public blockchain mainnet to keep the blockchain data manageable from the start.
- Spectrum is an Ethereum-compatible project.
  - Uses a new consensus (PoC) and block reward for SmartMesh ecosystem devices and IOT.
  - View the transactions on the BlockChain Browser Address (https://spectrum.pub/)

Spectrum Design Principles

- Reliabiliity must be maintained in unstable, underserved areas, in which Power and Internet connectivity is intermittent
  - Token transfers via Photon can operate with intermittent connection to the Spectrum blockchain; using the Photon state-channel secondary-layer architecture
  - MeshBoxes (running Spectrum and Photon) can operate with or without a grid connection; using renewable energy -- batteries and solar panel technology.
- Spectrum's consensus is lightweight and fair.
  - Proof of Capability runs on low-cost hardware such as MeshBox.
  - Staking of 880,000 SMT is required for a person to run a Spectrum mining node.
  - Good and bad behavior of nodes is taken into account in determining future block signers.
  - Future criteria include:
    - Whether the node is running on the MeshBox
    - Amount of resources shared with the community (Internet bandwidth, Mesh bandwidth, data storage and transactive energy)

© 2017-2019 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.

Mining Time Frames

- Slot
  - The time it takes for each successive block to be added to the blockchain
  - Nominally 14 seconds in the error-free scenario.
  - At the end of every Slot time, or 14 seconds, a new block should be added to the Spectrum Blockchain.

- Epoch
  - Each Epoch consists of 17 Slots.
  - With the start of each Epoch, the 17 Signers from the previous Epoch are released, and 17 to-be Signers for the current Epoch are selected.

© 2017-2019 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.

Spectrum Nodes

- **Staking node**: A Spectrum node which has staked 880,000 SMT and this thus able to earn Mining rewards

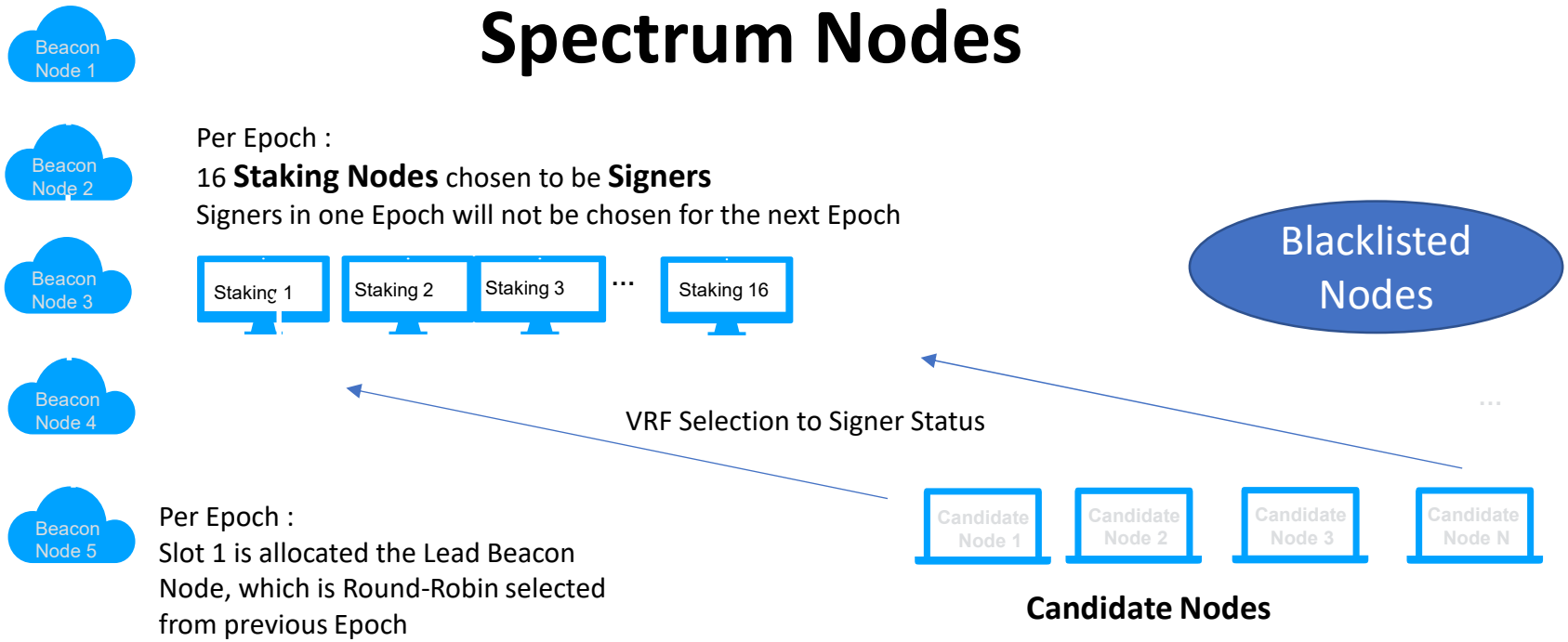
- **Beacon node**: A special Staking node, elected by the community to represent the interests of the entire community.
  - Beacon nodes will also sign blocks and earn tokens through mining.
  - Since the number of Beacon nodes (up to 5) is much fewer than that of Staking nodes (thousands), Beacon nodes benefit from higher frequency signing opportunities and thus mining rewards.

- **Miner Nodes:** Nodes which are capable of participating in the Spectrum Consensus process and thus earning Mining rewards. Includes both Staking and Beacon nodes

- **Full node**: Other nodes which maintain the blockchain data-structure, but have not staked 880,000 SMT, and are thus not qualified to be a Miner.

- The above Spectrum Nodes can take on the following **Status** during operation
  - **Signer Status**: Beacon nodes and Staking nodes which are chosen to sign blocks in a particular Epoch, and thus earn tokens through mining.
  - **Candidate Status**: A Staking node which is not chosen to be one of 16 signers in an Epoch and is waiting to be chosen in a future Epoch.

Spectrum Nodes



- Spectrum adopts a Two-Layer consensus architecture.
- Even if all Staking nodes are malicious, as long as all beacon nodes do not join them, Spectrum blockchain security can be guaranteed.
- When a Staking node is given the chance to sign a block, but fails, a Beacon node will take its place.
- Beacon nodes are selected by the SMT community, with POA mechanism as a transition consensus. As long as all these institutions do not conspire to be malicious, Spectrum is safe.
    - SmartMesh Foundation
    - SUSS
    - Blockchain Association Singapore
    - Huobi
    - One Beacon node allocated for UN.

Blockchain Signing Sequencing per Epoch

- Per Epoch, the first slot is allocated to a Beacon node.
- With five Beacon nodes, sequenced as {A, B, C, D, E}, the Lead Beacon node chosen for the current Epoch will be the next Beacon node in the sequence after the Lead Beacon node of the previous Epoch.
- If the Lead Beacon node fails to produce the correct block, the next Beacon node in the sequence will take its place; if this replacement Beacon node also fails, the next Beacon node in the sequence will step in, and so on.
- If all 5 Beacon nodes fail, the Spectrum blockchain processing pauses and waits until one of the Beacon nodes produces a correct block, at which point Spectrum continues operation.
- For a given Epoch, for slots 2 through 17, if a Staking node fails, the Lead Beacon node for that Epoch will be the first to try to produce the correct block.
  - If this Lead Beacon node fails to produce the correct block, the next Beacon node in the sequence will take its place; if this replacement Beacon node also fails, the next Beacon node will step in, and so on.

Block Attributes

- Block Difficulty Weight
  - Each block is assigned a difficulty weight.
  - For each slot, the block produced by a Signer (Beacon or Staking node) will be given the highest difficulty weight value (initially 6) of this height block. The height is the number of blocks currently on the blockchain.
  - If the Signer responsible for producing the block fails to produce the correct next block, the difficulty weight of the block produced by its substitute(s) will be decremented in order (5, 4, 3...).
  - In order to speed up the final result of the consensus, each Miner will proceed to append the next block on the blockchain branch with the highest difficulty weight value in total.

- Block Time Rules
  - The time to produce the next successive block and append to the blockchain is 14 seconds in the nominal case
  - However, the actual time could be between 14-34 seconds, in 4 second increments from the 14 second nominal case.
  - The first attempt for a new block is made 14 seconds after the previous block has been appended to the Blockchain.
  - If this fails, a replacement node, which is a Beacon node, produces a block 4 seconds later (at 18 seconds), and failing this second attempt, the third attempt being completed by 22 seconds, and so on, up to 34 seconds maximum.

Spectrum Epoch Execution Example

Slot:	1	2	3	4	5	6	7	…	17
Epoch N									
	Lead Beacon Node = B (fails) Difficulty=6 BT1= 14 sec	Miner 112 (succeeds) Difficulty=6 BT3= BT2 +14 sec	Miner 123 (succeeds) Difficulty=6 BT4= BT3 +14 sec	Miner 235 (fails) Difficulty=6 BT5= BT4 +14 sec	Miner 358 (fails) Difficulty=6 BT7= BT6 + 14 sec	Miner 5813 (fails) Difficulty=6 BT9= BT8 + 14sec	Miner 8132 (succeeds) BT11= BT10 + 14sec		Miner 1321 (succeeds) BT12= BT11 + (10*14)sec
	Beacon C (fails) Difficulty=5 BT= BT1 + 4 sec			Lead Beacon B (fails) Difficulty=5 BT= BT5 +4 sec	Lead Beacon B (succeeds) Difficulty=5 BT8= BT7 +4 sec	Lead Beacon B (fails) Difficulty=5 BT= BT9 + 4sec			
	Beacon D (fails) Difficulty=4 BT= BT1 + 8 sec			Beacon C (succeeds) Difficulty=4 BT6= BT5 +8 sec		Beacon C (succeeds) Difficulty=4 BT10 = BT9 + 8sec			
	Beacon E (fails) Difficulty=3 BT= BT1 + 12 sec			Beacon D (succeeds) Difficulty=3 BT6'= BT5 +12 sec					
	Beacon A (succeeds) Difficulty=2 BT2= BT1 + 16 sec			In Slot 4, both C and D produced a block. However, all nodes will choose the block from C since it had the higher Difficulty weight (4 for C, versus 3 for D)					
Epoch N+1									
	Lead Beacon = C (fails) Difficulty=6 BT13= BT12 + 14sec	Miner 512 (succeeds) Difficulty=6 BT15= BT14 + 14sec	Miner 529 (succeeds) Difficulty=6 BT16= BT15 + 14sec	Miner 6210 (succeeds) Difficulty=6 BT17= BT16 + 14sec	Miner 858 (fails) Difficulty=6 BT18= BT17 + 14sec	Miner 437 (fails) Difficulty=6 BT20= BT19 + 14sec	…	…	…
	Beacon D (fails) Difficulty=5 BT=BT13 + 4sec				Lead Beacon C (fails) Difficulty=5 BT= BT18 + 4sec	Lead Beacon C (fails) Difficulty=5 BT= BT20 +4sec			
	Beacon E (fails) Difficulty=4 BT=BT13 + 8sec				Beacon D (succeeds) Difficulty=4 BT19= BT18 + 8sec	Beacon D (fails) Difficulty=4 BT= BT20 +8sec			
	Beacon A (fails) Difficulty=3 BT=BT13 + 12sec					Beacon E (succeeds) Difficulty=3 BT21= BT20 +12sec			
	Beacon B (succeeds) Difficulty=2 BT14=BT13 + 16sec								

Spectrum Node Operation Around Error Scenarios

- Error scenario 1: The node responsible for the block is not able to produce the block.
  - If, in a slot time, the node responsible for the block is not able to produce the block, one of the Beacon nodes will produce the block.
- Error scenario 2: The Spectrum node receives a block with inconsistent parent block
  - If a node receives a newly mined block, whose parent block is inconsistent with that of the main branch, the node will decide on the branch which has the highest total Difficulty weight.
- Error scenario 3: The Spectrum node receives a plurality of blocks, each of whose parent is the latest block on the main branch.
  - Due to non-uniform latency in communication between nodes, and other potential distributed computing issues, a Spectrum node may receive multiple blocks, such as one from the designated miner (in slots 2 through 17 of an Epoch) and also one or more from a Beacon node.
  - The Spectrum node will choose the block which has the highest Difficulty weight, which will be the block with the earliest time.
- Error scenario 4: The Spectrum node receives multiple blocks, in which there are two or more branches from the latest parent block on the main chain.
  - The node adds up the difficulty of each branch, and chooses the branch which has the highest sum of the Difficulty weights.
  - For instance, the latest parent block is at height N, and the received blocks form two different branches. One branch consists of two blocks (at height N+1, and N+2) whose Difficulty weights are 1 and 4, and the other branch consists of one block (at height N+1) with Difficulty weight 6.
  - Then the second branch with the one block will be chosen since the Difficulty weight is 6, versus 5 (=1+4) for the other branch.

(Malicious) Double Spend Attack Analysis

- A Malicious actor tries to spend the same crypto-currency (tokens) multiple times.
- Attacker executes a transaction (such as spending tokens or lying about how many resources (computing, cryptocurrency resources, etc.) which the attacker has contributed).
- Then, the attacker attempts to roll back the transaction, so that the transaction is never recorded in the blockchain.
- Attack steps:
  - First the attacker submits a transaction (to be later rolled back) to the whole network, and continues mining on the fork of the previous block (excluding the fork of the transaction to be rolled back) until the transaction is confirmed by n blocks.
  - If the number of blocks on the (wrong) fork becomes more than n, the attacker announces the block containing the transaction to be rolled back.
  - Then, since the length of the bifurcation chain is larger than the original main chain, the whole network node regards the (wrong) bifurcation chain as the main chain. At this point, the transaction is rolled back and double-spending has occurred.
- With the two-tiered Beacon and Staking node hierarchy
  - If all beacon nodes become malicious and unite to commit crimes, a Double-Spending attack can be successful.
  - If the beacon nodes are not malicious, no matter what percentage of mortgage nodes are malicious, they cannot succeed in a double-spending attack.
- As for the case of some Beacon nodes and some Miner nodes being malicous
  - A double-spend attack, while possible, is still very difficult to achieve due to the VRF random selection of Miner nodes for each Epoch.
  - Also, Beacon nodes are chosen from the list of reputable organizations and close partners to SmartMesh and MeshBox, so there is very little chance for a Beacon node to be malicious.

Other Malicious Attacks

- Sybil Attack
  - The Sybil attack occurs in the P2P network.
  - Because a Miner node can join and exit at any time, in order to maintain network stability, the same data usually needs to be backed up to multiple distributed nodes.
  - The same malicious node can have multiple identities.
  - Each node's data is spoofed backed up to the same malicious node.

  - However, to be a Signer on the Spectrum blockchain, it is necessary to stake 880,000 SMT.
  - Because of this high threshold, it is very costly to create new Signer nodes, and therefore it is very expensive to be able to stage a Sybil Attack.

- DDOS
  - A Distributed Denial of Service attack can cause a node to fail to process normal data.
  - The attackers send a large amount of data to the node (such as sending a large number of small transaction requests and adjusting the gas charges) so that the system cannot handle normal transactions.

  - Since the node transaction pool (TxPool) limits the number of local transaction caches, this limits the number of accounts sent by the cache and the maximum number of transactions sent per account.
    - Thus, to a large extent, the risk of DDOS attacks is reduced.
  - However, due to the relatively low price of SMT, the gas handling fee is relatively low, so it is still possible to create a large number of accounts, and each account may send many transactions to cause network congestion.
  - Solutions include raising the gas fee, and incentivizing users to use the Photon Payment network for most transactions.
    - Photon has higher TPS, is much faster in terms of transaction confirmation latency and can be made cheaper, in terms of fees, than a Spectrum transaction.

Blockchain Comparison

	Blockchain Consensus Algorithm	Smart-Contracts Support	Scalability Strategy	Transactions per Second (TPS)	Latency = Consensus time	Cross-Chain support	Transaction Fee
Bitcoin	POW. Very heavy (CPU, GPU, Memory, Disk) and expensive in terms of money and power.	Not generally RSK working on Solution	State-Channel with Lightening, in commercial use.	7	6 block times (1 hour)	No	~ $1 USD
Ethereum	POW Plan to move to Casper Proof of Stake, but no timeframe.	Yes	State-Channel with Raiden, but not working yet. Plasma, not ready.	9.5	12 block times (3 minutes)	No	~ $0.04 to 0.21 USD, which is at least 32,000x more expensive than Spectrum
Ethereum Plasma	Root Chain consensus used, and Child chains have multiple options.		Hierarchy of Child Chains operating in parallel	Scales with the number of Child Chains	Depends on consensus of Child Chain.	Yes	Deposit into Plasma Root Chain needed.
Hyperledger	Various, such as Permissioned Voting and BFT (Fabric), and PoET (Sawtooth)	Yes	Centralized, so not scalable.	100s to 1000s Goal of 100,000	Voting: The more nodes, the more time required for Consensus	No	0 (no incentive to use)
EOS	DPOS	Yes	21 super nodes	1000s	15 block times (1.5 seconds)	No	0 (subject to depreciation, endless issue of 5% additional tokens per year, leads to inflation)
SmartMesh Spectrum	Proof of Capability: Round-Robin amongst a group of 17 Signers, which are continuously rotated through a pool of Miner nodes during an Epoch (17 block times). Very light, runs on Mobile CPU. Photon runs on Smartphones	Yes	Photon Network State Channel for Direct Peer-to-Peer (Smartphone to Smartphone) and Mediated Transfers through other Photon Nodes. Highly scalable with the number of nodes due to P2P concurrent transfers.	Spectrum: 16 Photon: 100,000s to 1,000,000 and beyond	14 block times (3 minutes) Photon Payment transfer finality is 1 second. Can be done offline (not connected to Spectrum).	Yes	~ $0.00000126 USD = 0.0004 SMT Photon is Free for Direct Transfers

The number of people living on less than $1.90 a day [is] 736 million (10% world's population) [World Bank 2015].

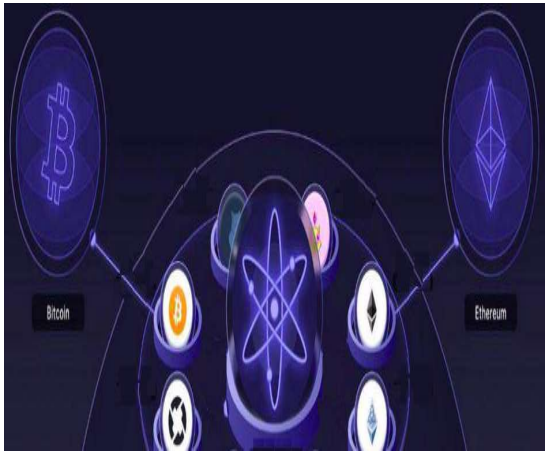
© 2017-2020 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.

Atmosphere
Deep Dive

SmartMesh

Atmosphere Deep Dive

What is cross-chain?

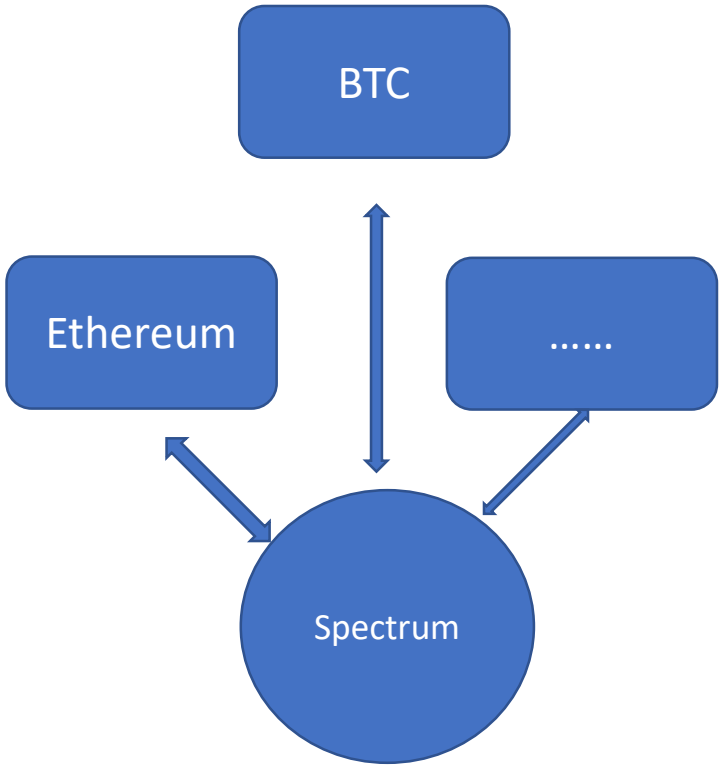


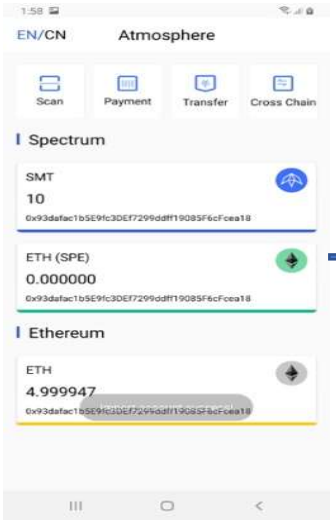
- Cross-chain operation involves transferring information and data from one chain to another.
- Often, assets on one chain are exchanged for assets on another chain.
- Cross-chain technology is a bridge, for the interconnection and intercommunication of information and value between two blockchain.

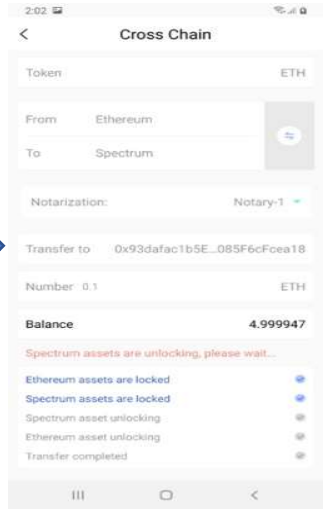
Why do we need to cross-chain?

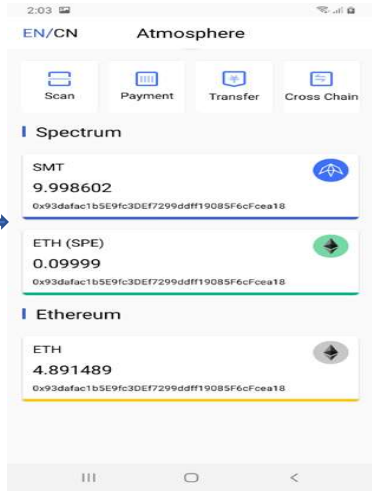
- Asset exchange on different chains, namely atomic transactions
- Token exchange through multiple scenarios
- Smart contracts spanning multiple blockchain networks
- Cross-chain investment of value-added services for assets on different chains

SmartMesh CrossChain with Atmosphere

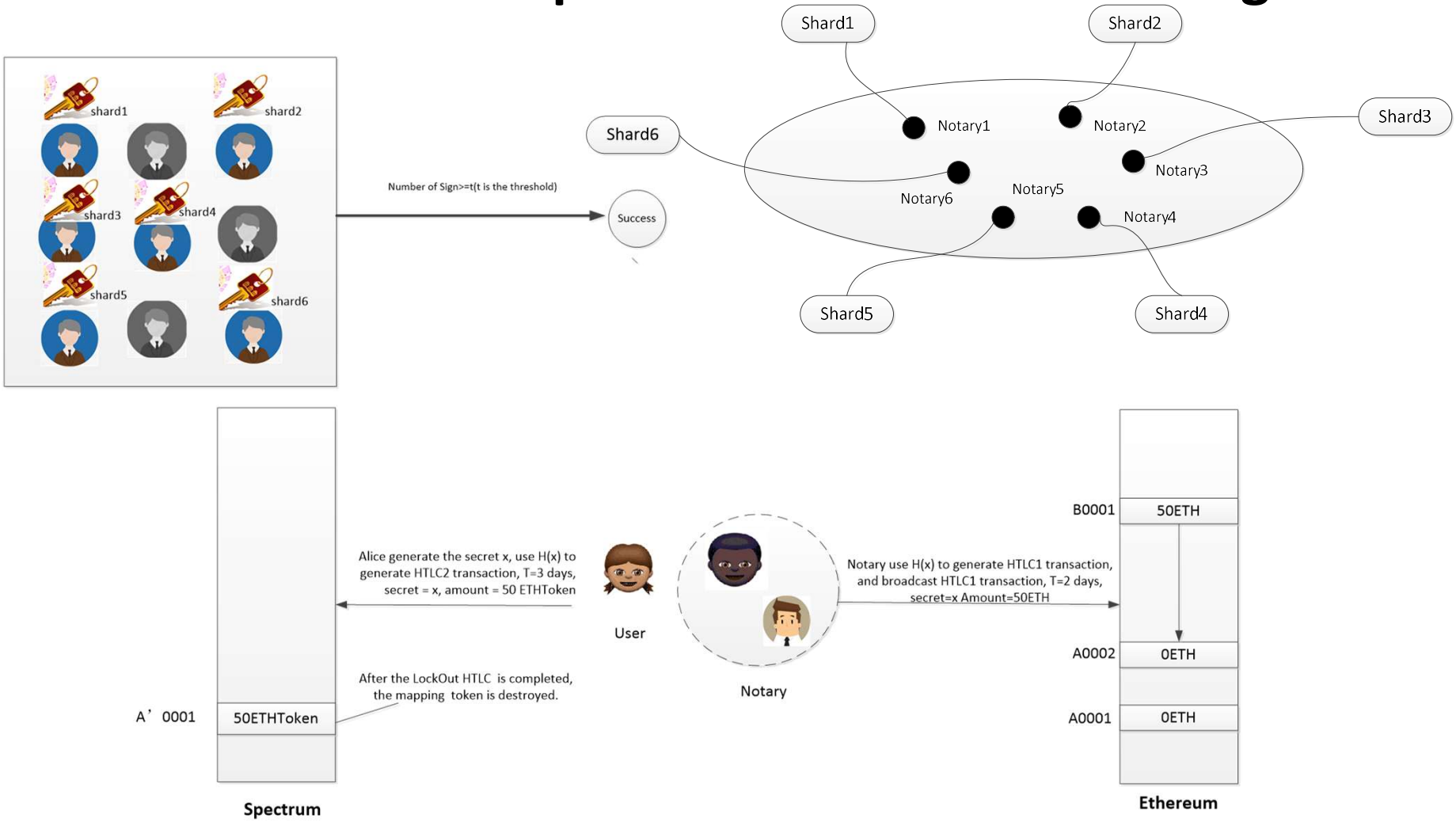






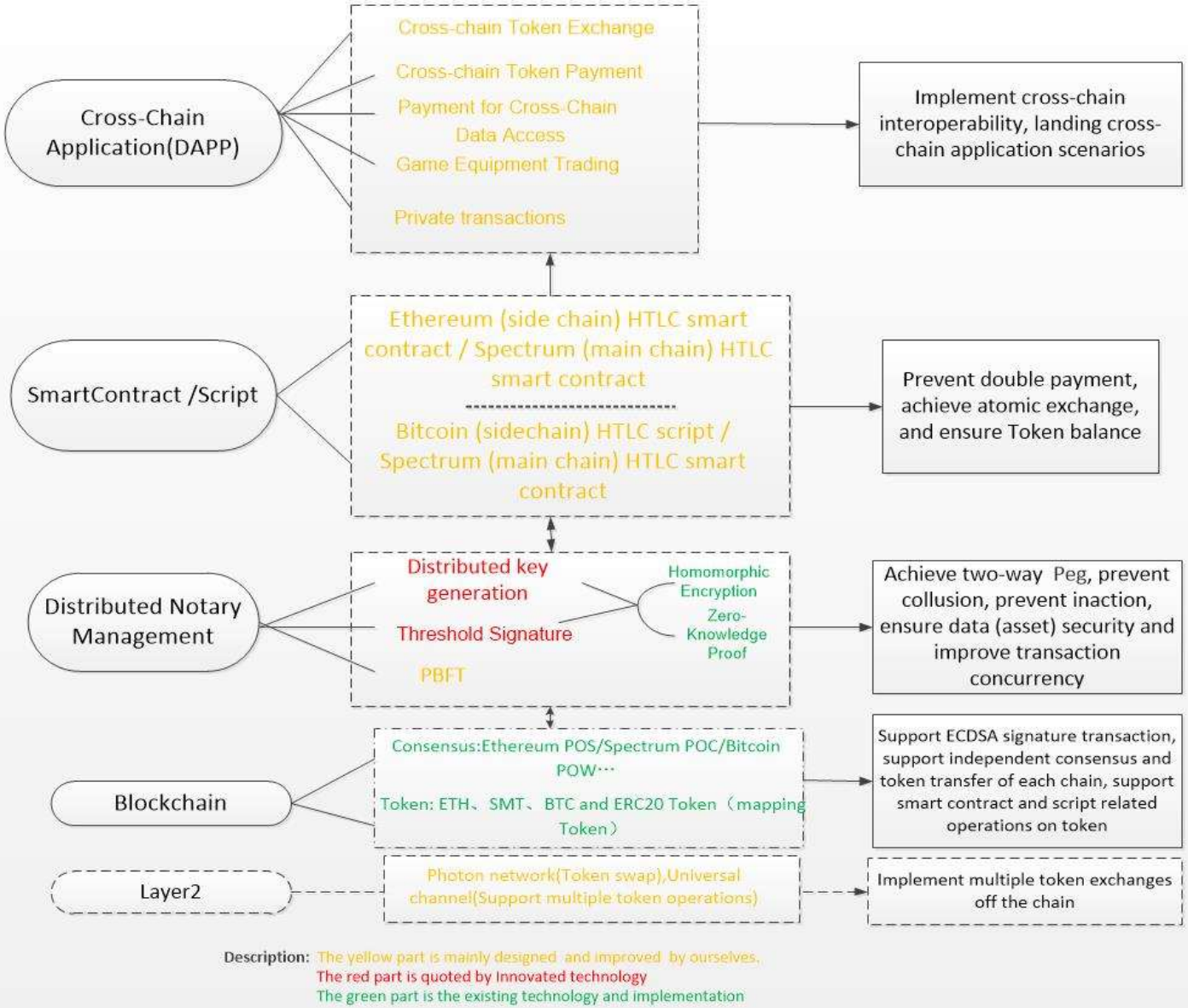


SmartMesh Atmosphere Crosschain Technologies

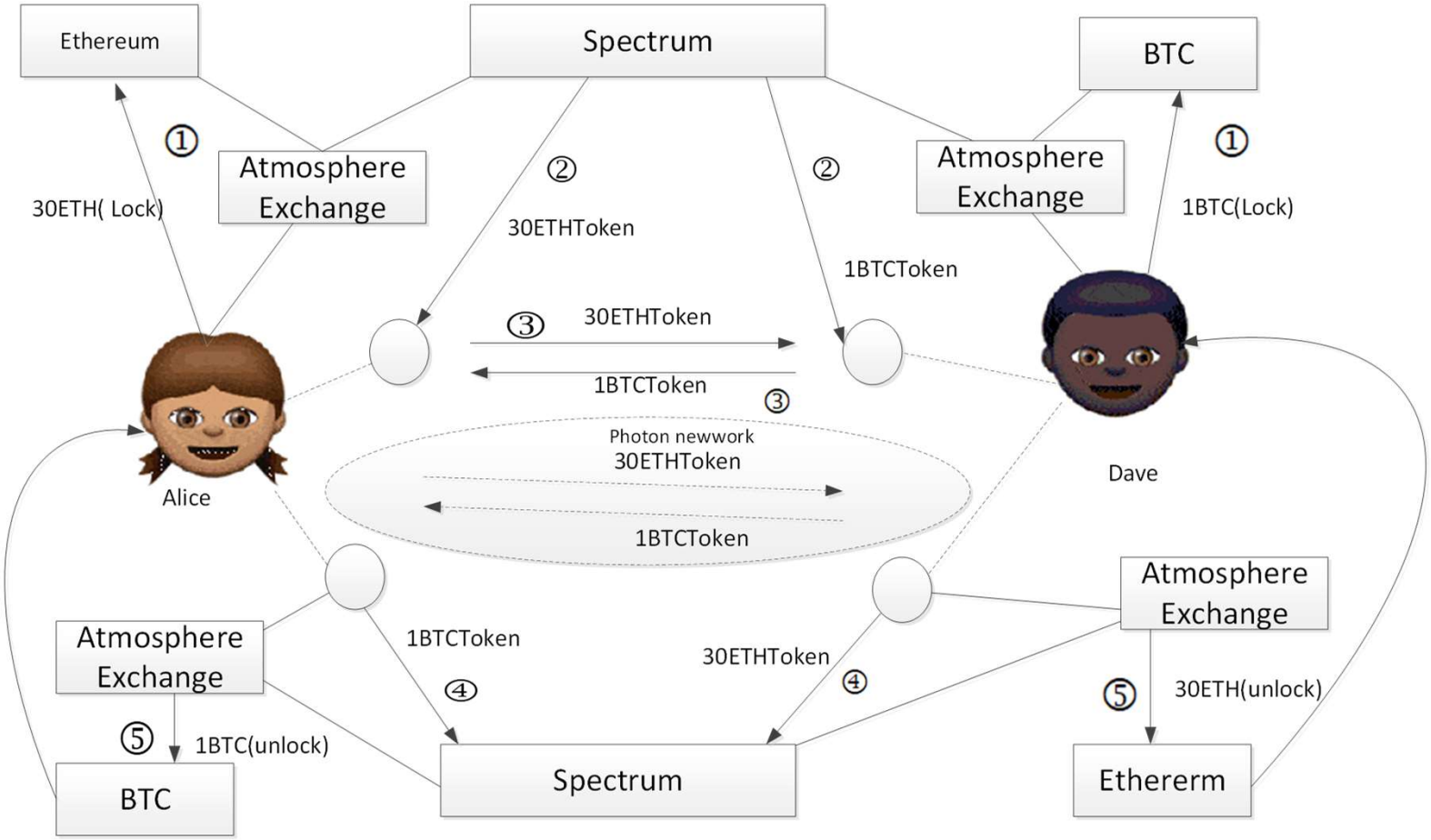


- **Distributed Key**: Reduce the risk of private key disclosure and multiple notaries staging joint malicious attacks
- **HTLC Atomic Interchange**: Guarantee that the cross-chain transaction is either successful or fails, and does not allow loss of tokens for users
- **Threshold Signature**: Improve the success rate of the transaction and prevent the not-acting attack of an individual notary
- **Zero-Knowledge Proof:** Ensure the security of the transaction
- **PBFT**: Solve the distributed consistency problem of nonce and UTXO management by multiple notaries

The Architecture of Atmosphere



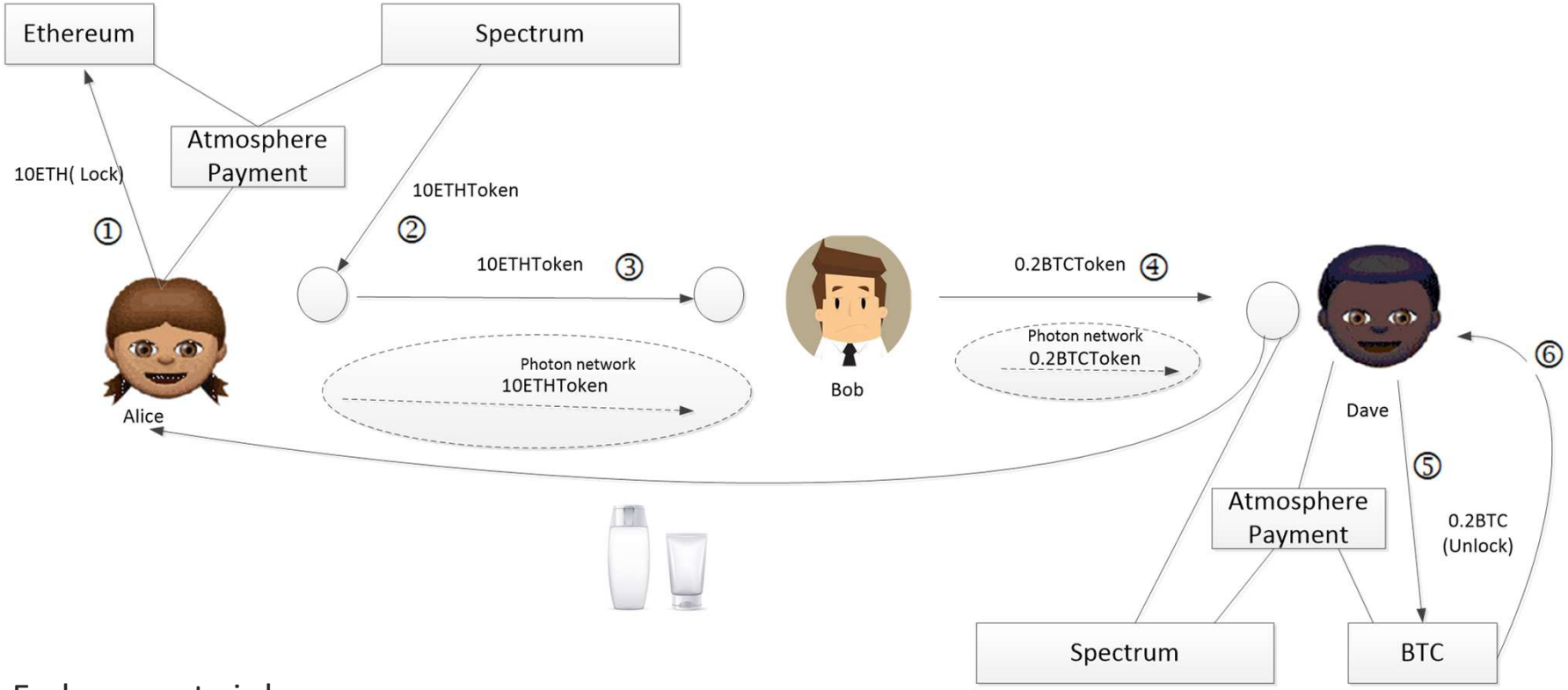
Scenario 1: Crypto-Currency Exchange via Atmosphere



- Exchange rate is known (example)
  - 30 ETH = 1 BTC
- Alice locks 30ETH, and the 30 ETHToken is generated on Spectrum
- Dave locks 1BTC, and the 1 BTCToken is generated on Spectrum
- ETHToken and BTCToken are atomically exchanged either
  - ON-CHAIN (SPECTRUM) OR
  - OFF-CHAIN (PHOTON)
- After the exchange, each mapped currency is unlocked. Thus, a successful currency exchange has occurred.
  - ALICE RECEIVES 1 BTC AND
  - DAVE RECEIVES 30 ETH

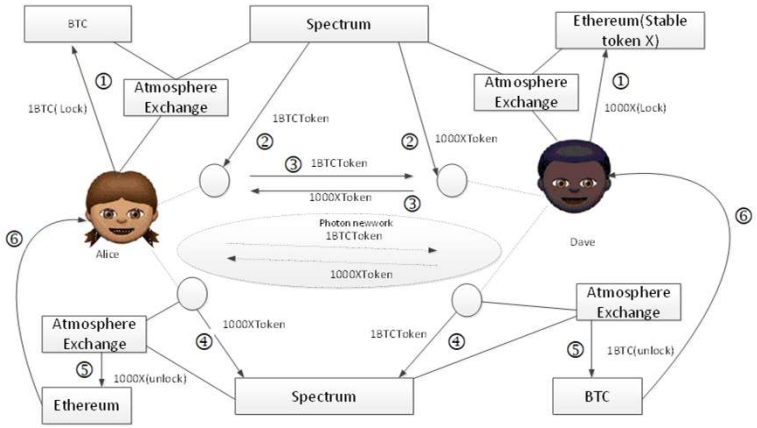
© 2017-2019 SmartMesh Foundation Pte. Ltd., MeshBox Foundation Pte. Ltd.

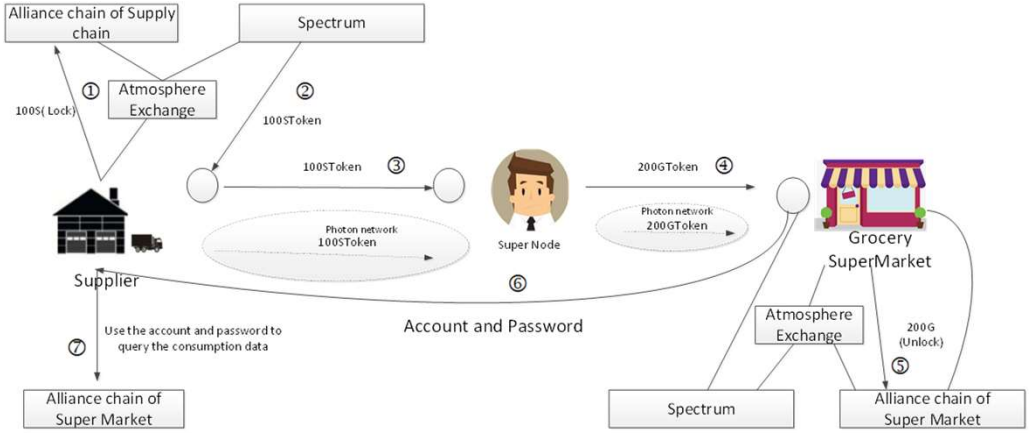
Scenario 2: Cross-chain Token Payment via Atmosphere

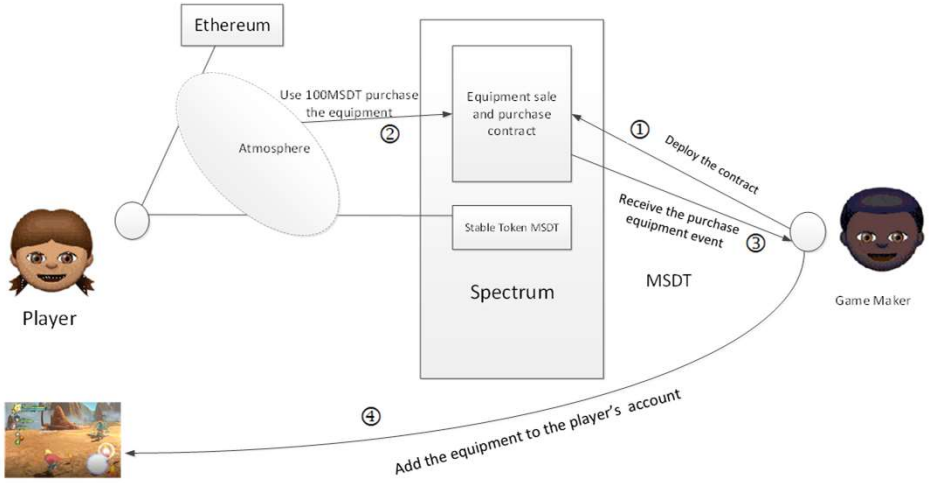


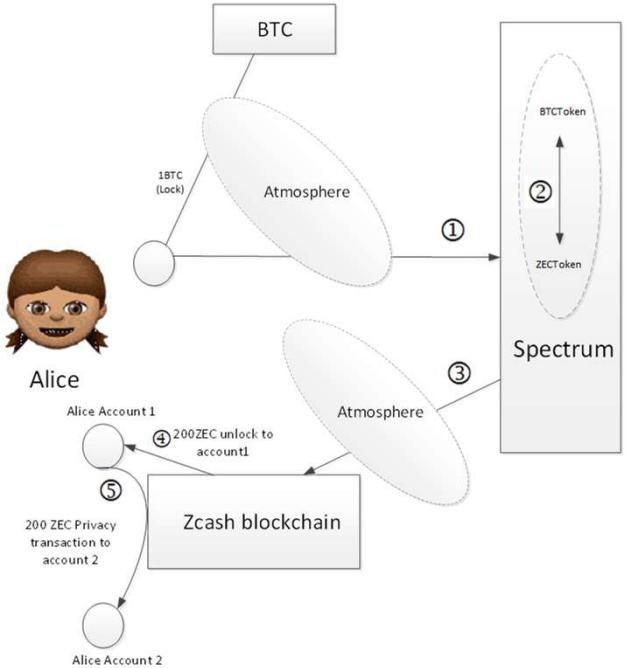
- Exchange rate is known
  - 10 ETH = 0.2 BTC
- Alice plans to buy moisturizer with ETH
- Alice locks 10ETH,and the 10ETHToken is generated on Spectrum
- Alice atomically pays to Super-node Bob
- Bob atomically pays manufacturer Dave
- Alice gets the moisturizer and Dave receives the 0.2 BTC
- Atomic exchanges can happen either
  - ON-CHAIN (SPECTRUM) OR
  - OFF-CHAIN (PHOTON)

Other Scenarios

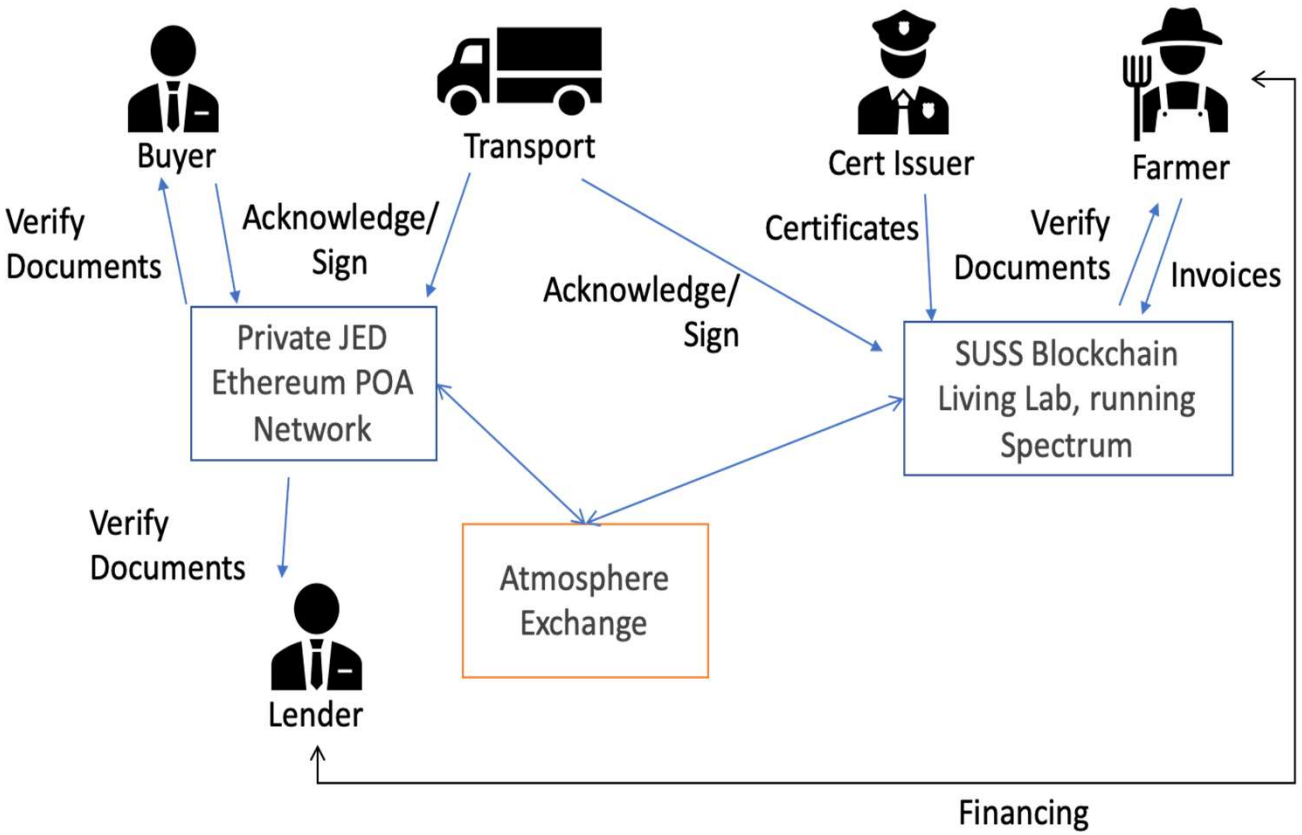








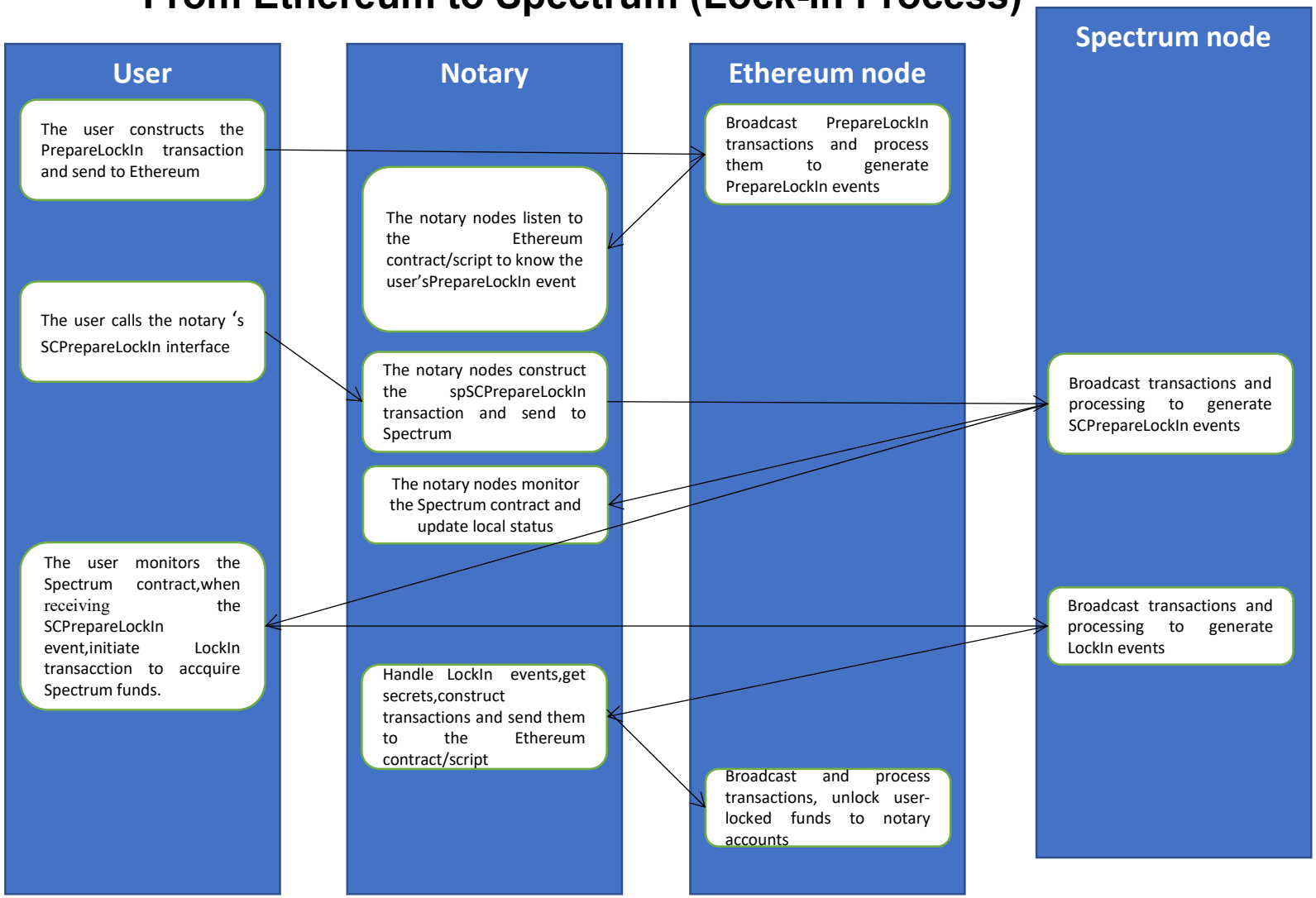
Jedtrade Interoperability with SmartMesh Eco System



Atmosphere DEMO

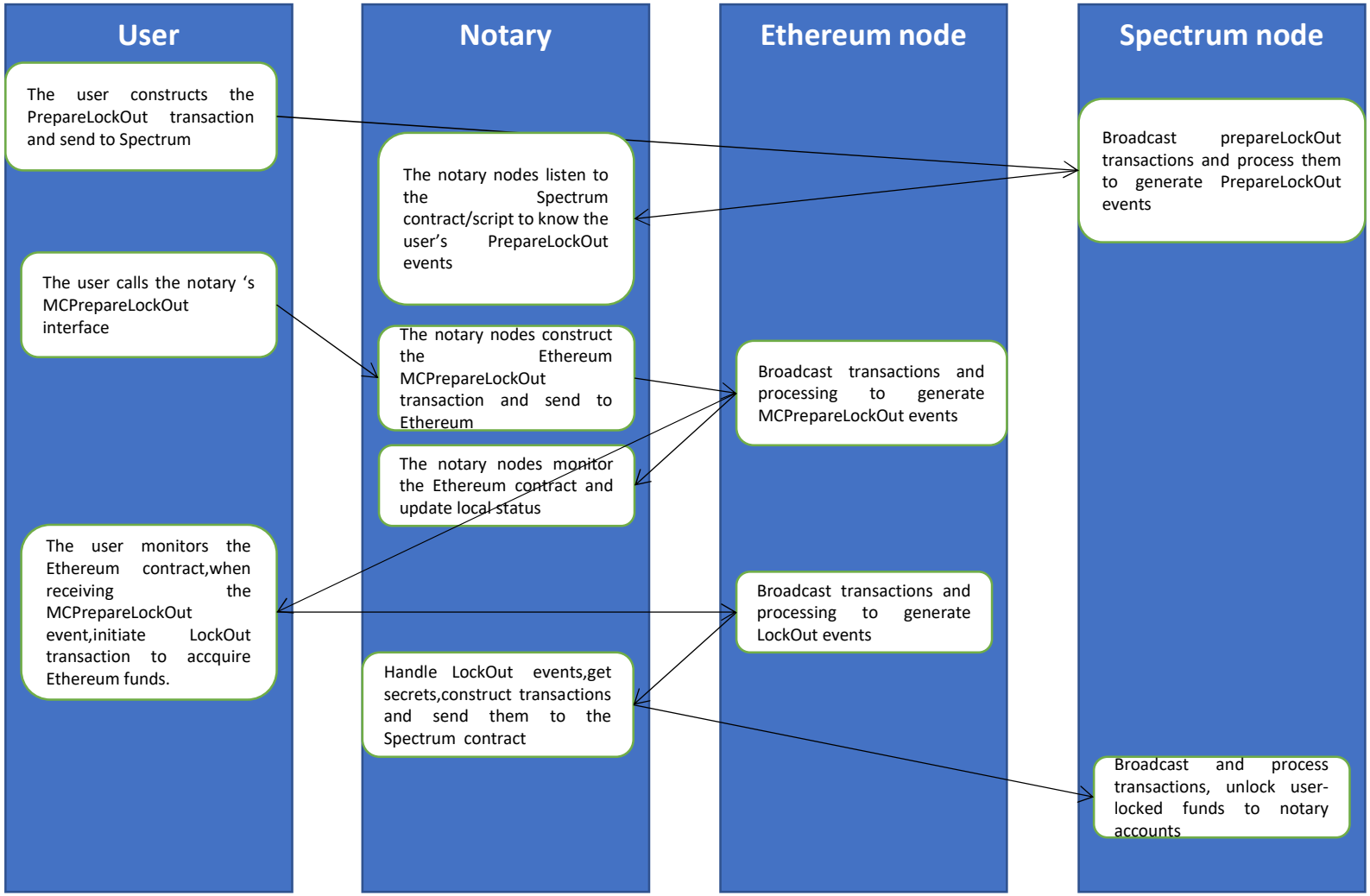
Atmosphere Crosschain Process

- **From Ethereum to Spectrum (Lock-In Process)**



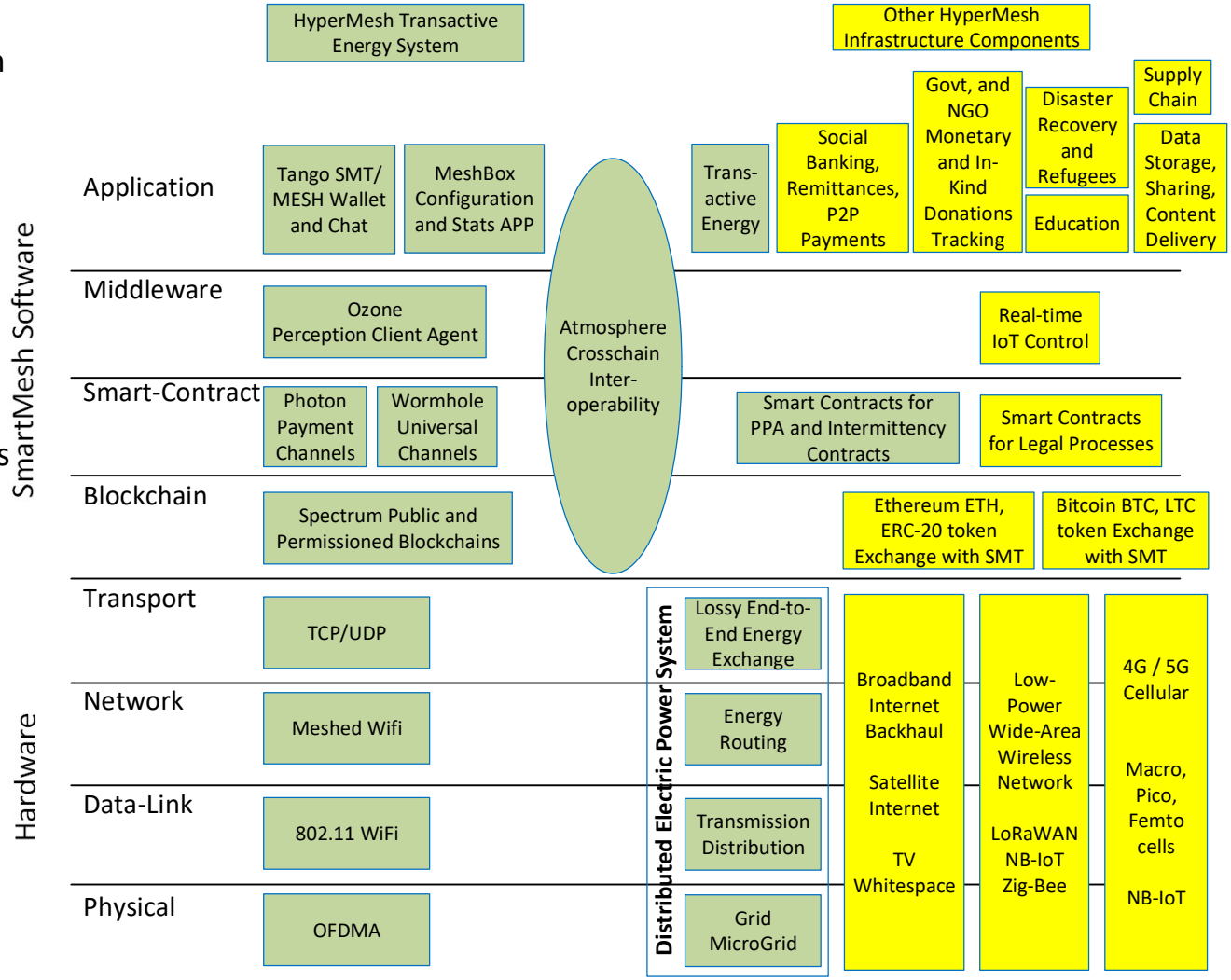
Atmosphere Crosschain Process

- **From Spectrum to Ethereum (Lock-Out Process)**



HyperMesh Protocol Stack on SM and MB Platform

- Applications
  - Atmosphere Cross-Chain
  - Energy Routing and Trading Algorithms based on AI, ML
  - IoT Monitoring and Control
  - Secured Data Storage and Communications
  - Air/Sea Port Applications
- SmartMesh Blockchain, Smart-Contracts, Photon
- Distributed Electric Power System (NTU)
- MeshBox Hardware
  - Edge/fog communications and computation
  - IoT Gateways and Terminals



© 2017-2020 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.

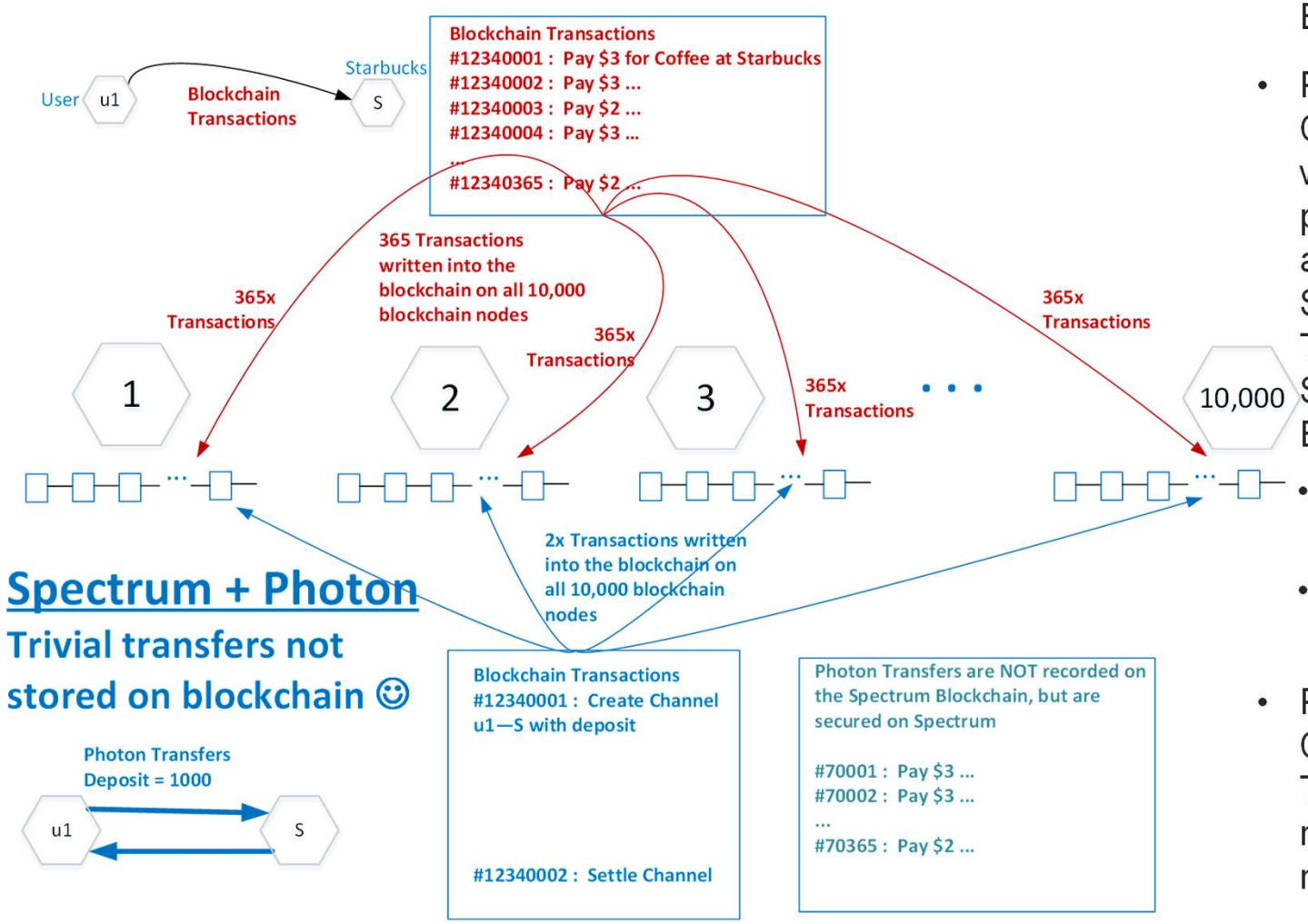
Photon Differentiation

- Photon Synergy with Spectrum: Photon Offloads most transactions from Spectrum
- Off-chain Payment Network for Intermittent Internet Access
- Lightweight, running on Smart Device
- Low-latency finality of Transfer (1 sec)
- High Transactions-per-Second (TPS) throughput with concurrent Peer-to-Peer transfers
- Synergy with MeshBox Mesh Network (providing a super-highway of payment routes)

Synergy : Spectrum + Photon

Blockchain ONLY

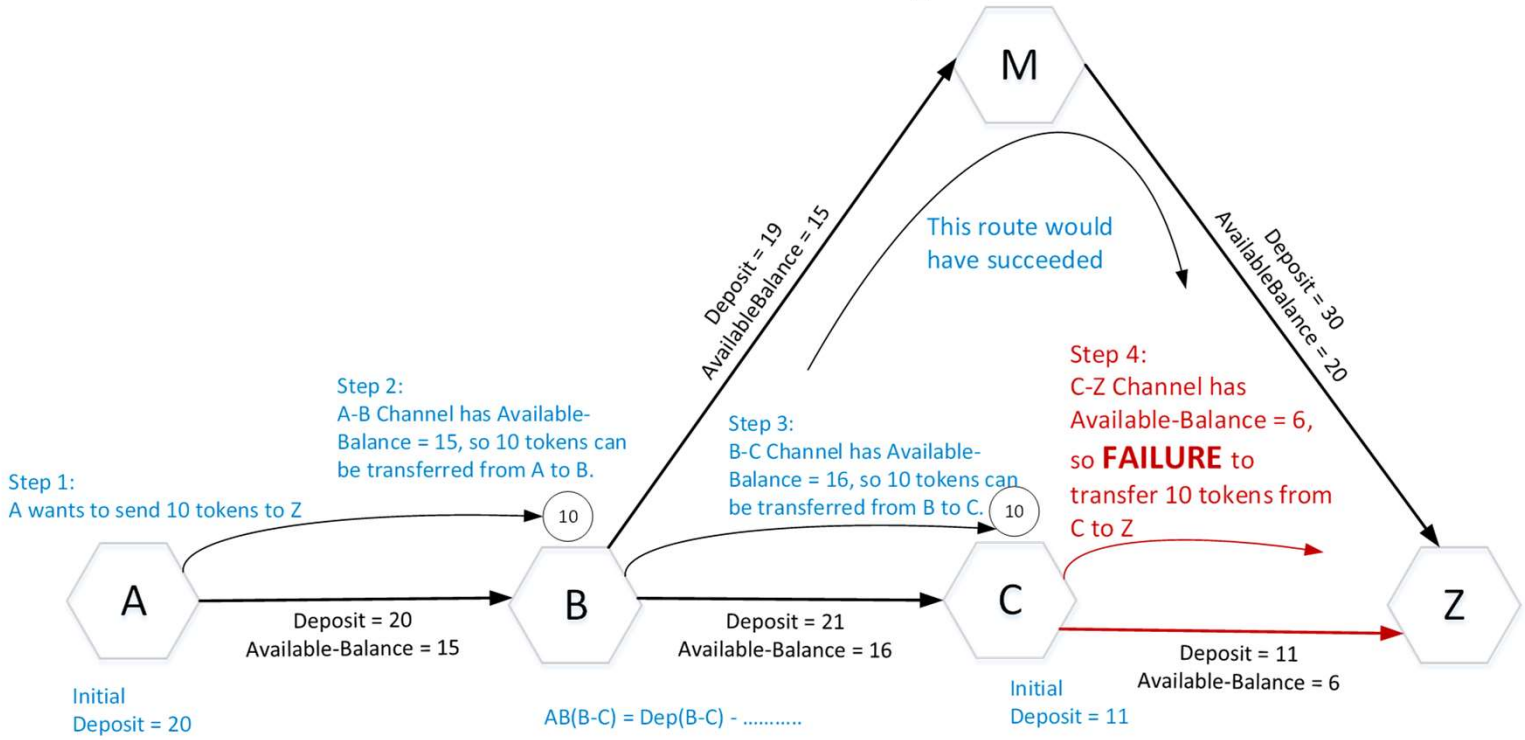
(Large amount of trivial information is stored on all nodes, forever ☹



- Photon for Spectrum is analogous to Lightning for Bitcoin and Raiden for Ethereum
- Photon is a Smart-Contract on Spectrum which execute in parallel (peer-to-peer) and thus do not impact Spectrum Transactions-per-Second (TPS)…. Except:
  - Initial Deposit onto Channel
  - When Channel is settled.
- Photon transfers are CONCURRENT, so TPS scales with the number of Photon nodes to Millions+

© 2017-2019 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.

Issues with Conventional Payment Networks



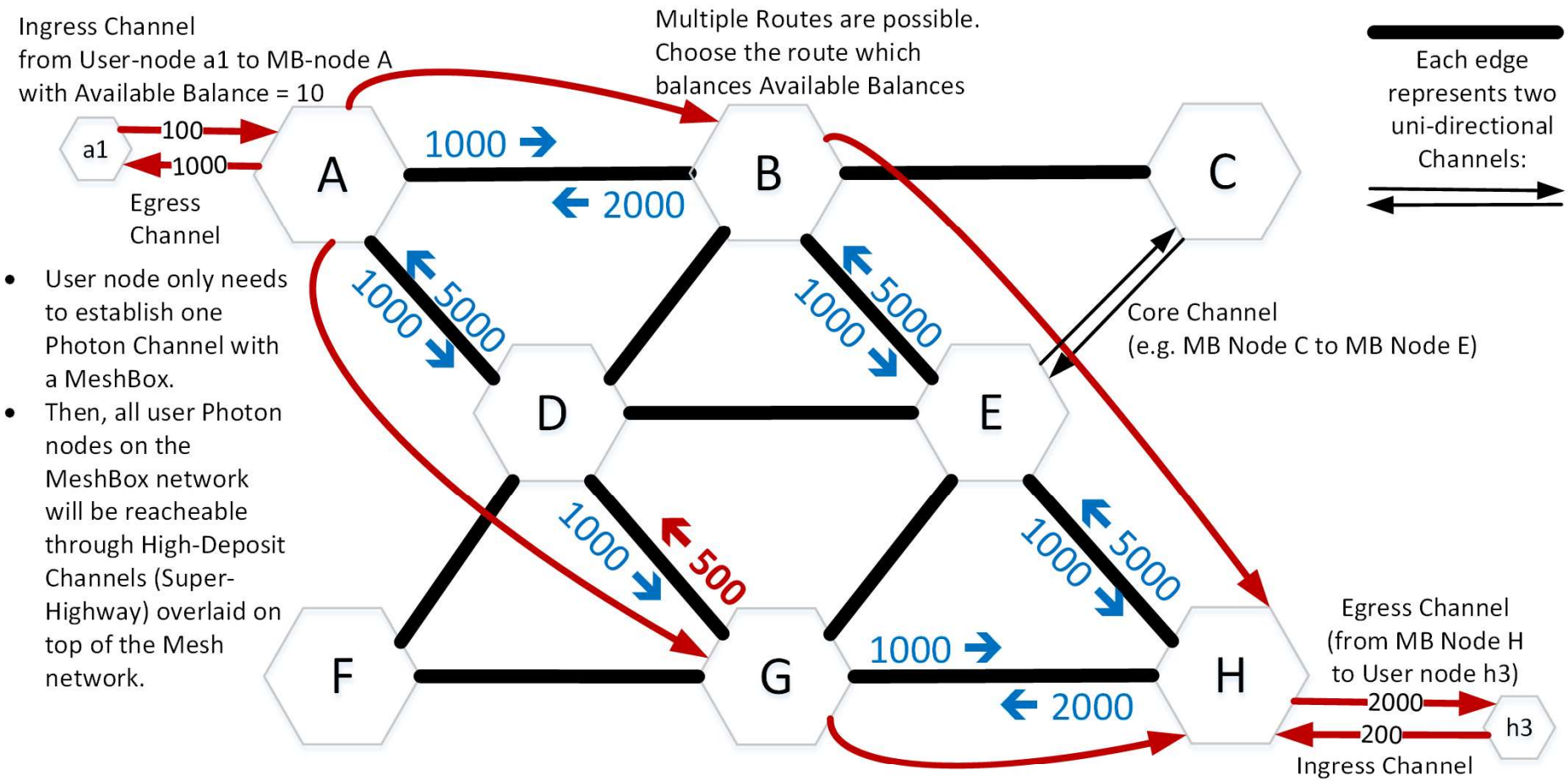
Payer-A wishes to transfer tokens, through Photon, to Payee-Z

- Bitcoin Lightening and Ethereum Raiden are conventional Payment Networks.
- A transfer is successful when a Route can be found from Payer (A) to Payee (Z)
- Conventional Payment Networks are usually User Defined, with **small deposits** on each Channel
- Routing from Payer to Payee has high chance to FAIL
  - **Complicated Topology**
  - **Inadequate Available-Balance** on links results in **no feasible route**
- Only **small Payments are supported** due to small user-defined Channels.

Conventional Payment Networks (Bitcoin, Ethereum) suffer from narrow Channels and high routing FAILURES

© 2017-2019 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.

Synergy : Photon + MeshBox



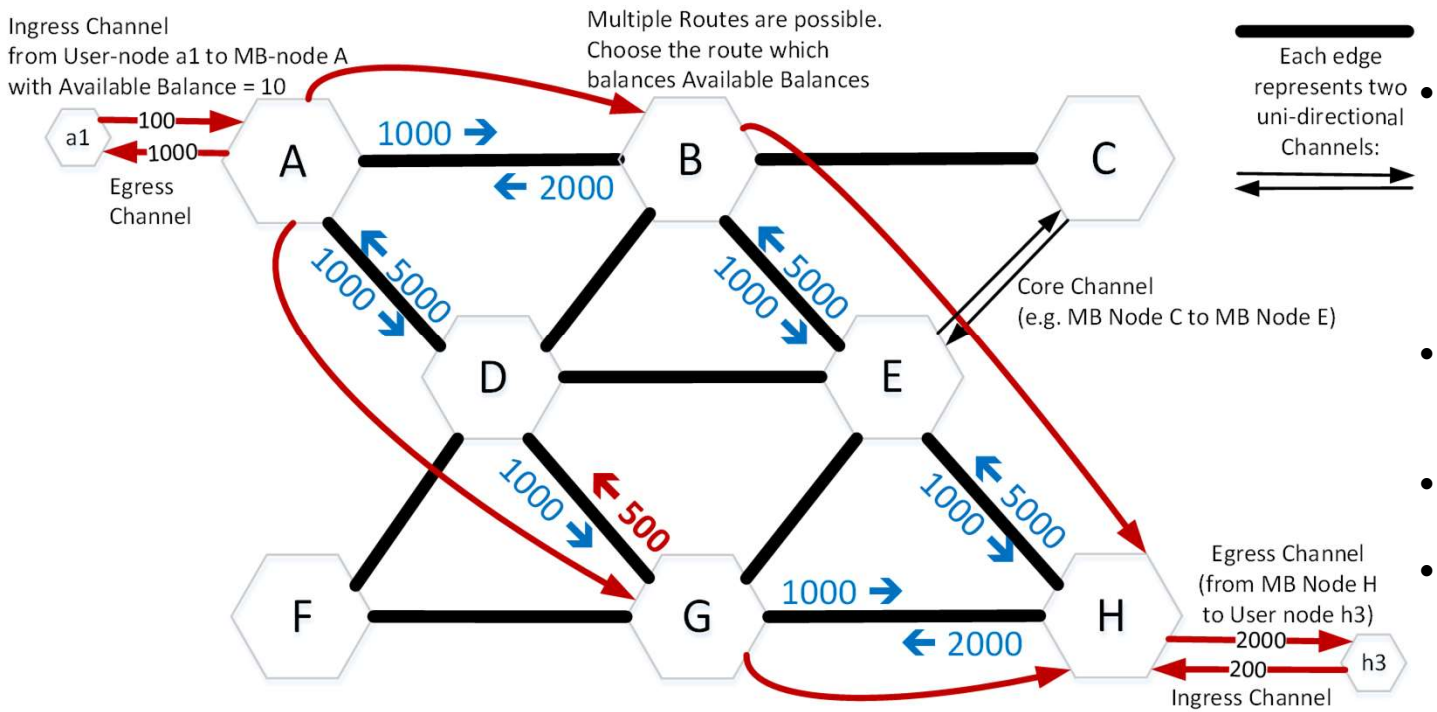
- User node only needs to establish one Photon Channel with a MeshBox.
- Then, all user Photon nodes on the MeshBox network will be reacheable through High-Deposit Channels (Super-Highway) overlaid on top of the Mesh network.

- MeshBoxes are Photon nodes with large Deposits on Channels
- Routing through Topology is simplified
- Large Deposits reduces routing failures
- Large transfers are supported

MeshBoxes support Wide Photon Channels which increases Token Routing Success

© 2017-2019 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.

Smartmesh Photon secondary layer

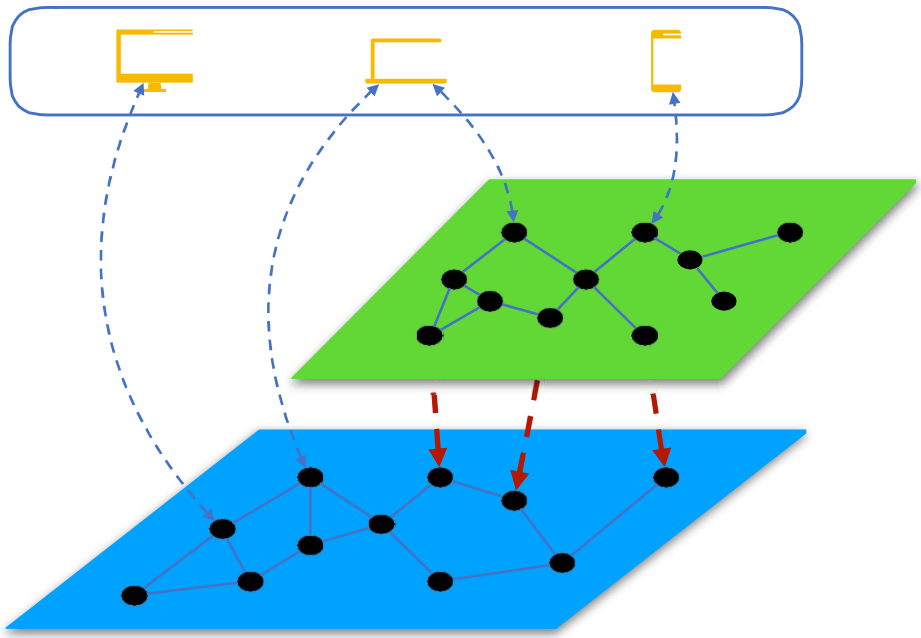


- At Creation, each Channel has a Deposit (=D), which is recorded on the Spectrum blockchain.
- When a Channel is settled, each side gets what is due.
- A gets AvailableBalance(A_B)
- B gets AvailableBalance(B_A)

- At initialization, each Channel has a Deposit (=D), which is recorded on the Spectrum blockchain.
- AvailableBalance of the Channel from A to B (A_B) is a function of
  - X(A_B) = Sum of all DirectTransfer amounts, which is the amount which A owes to B directly. Initial value = zero.
  - X(B_A) = Sum of all DirectTransfers which B owes to A directly.
  - Y(A_B) = Sum of all LockedTransfer amounts for mediated transfers from A to B (e.g. a transfer a1—A—B—E—H—h3), which are the locked amounts of MediatedTransfers which may or may not succeed.
  - Y(B_A) = Sum of all LockedTransfer amounts for mediated transfers from B to A.
- AvailableBalance of the channel (A_B) = D – X(A_B) + X(B_A) - Y(A_B)

© 2017-2020 SmartMesh Foundation Pte. Ltd. | MeshBox Foundation Pte. Ltd.

Blockchain Layer2 State Channel Expansion

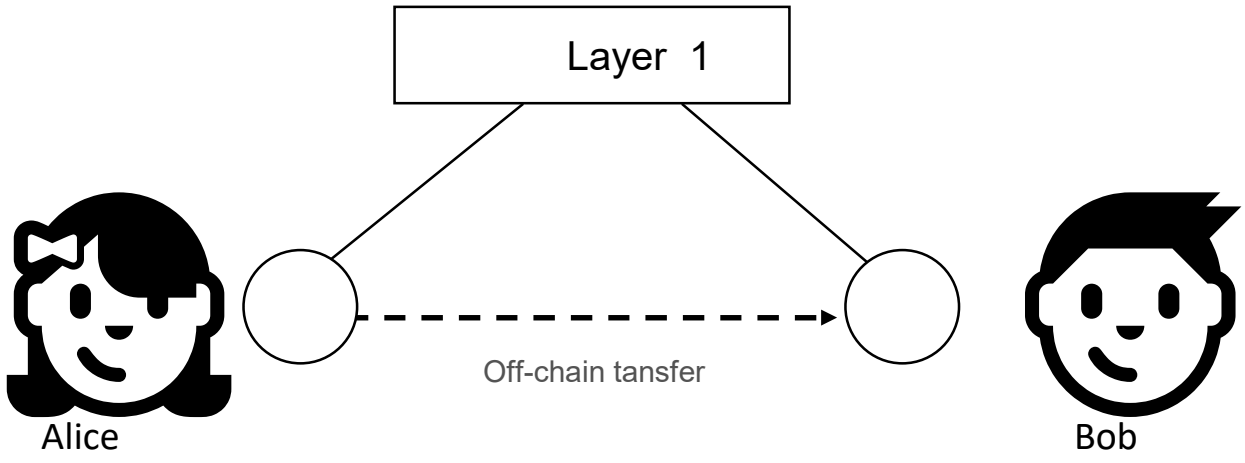


Application**(End Point):**
Browser/ Wallet/ DApp(s)

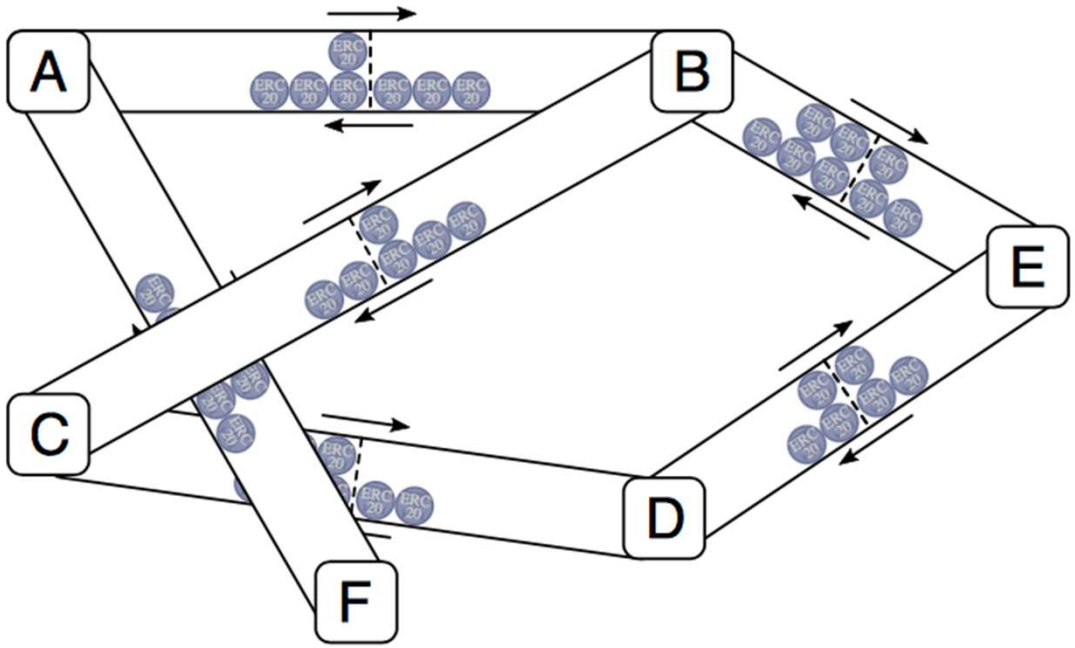
Layer2:
State Channel

Layer**1:**
Bitcoin / Ethereum/
Spectrum/EOS

What is a State Channel?

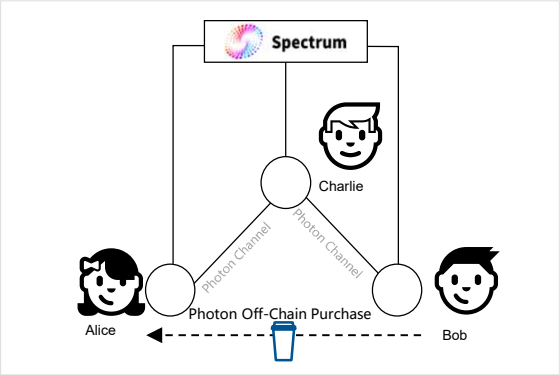


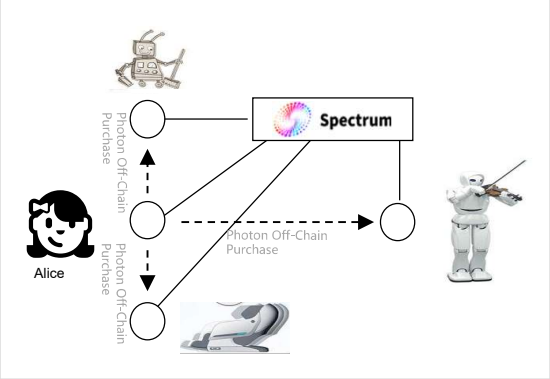
State Channel Use - Micropayments

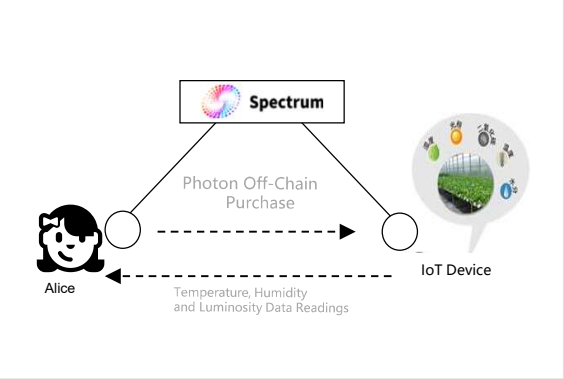


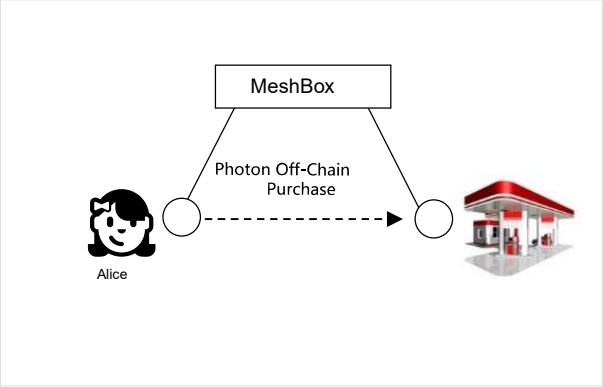
Photon Network

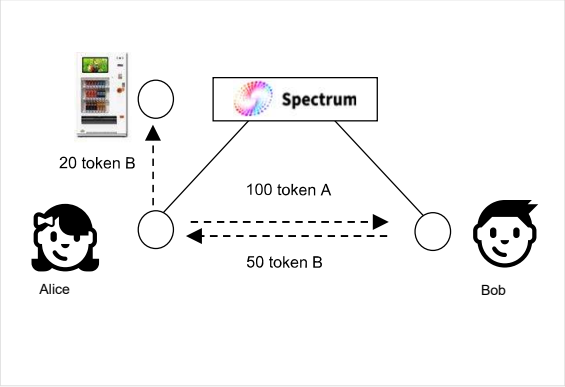
The Photon Network makes payments possible both on and offline from the Spectrum blockchain with total security, speed, scalability and low cost， and can satisfy multiple types of off-chain payment scenarios.





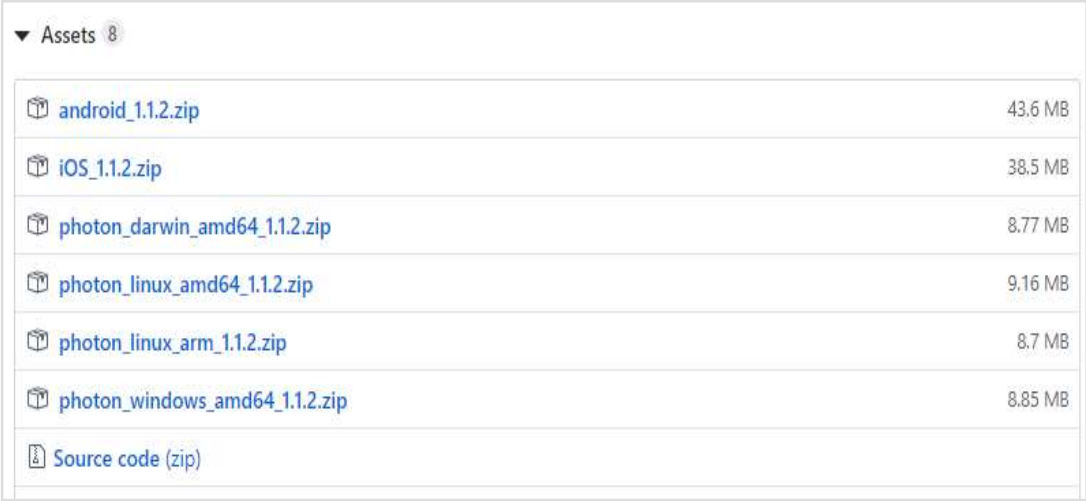






Photon Network Supported Platforms

- All Platforms are Supported
- Windows， Linux， Mac， Android， iOS

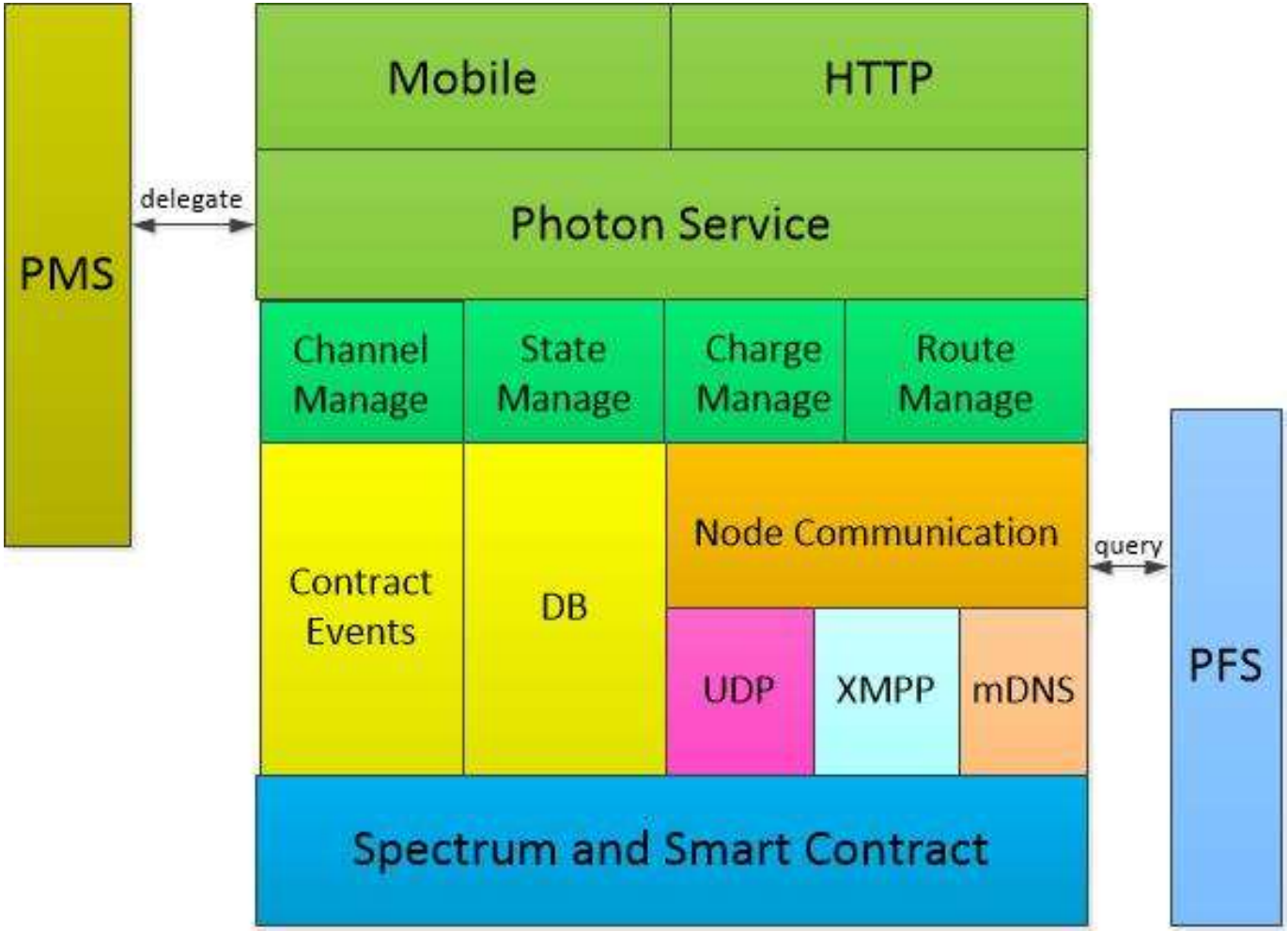


Assets 8

android_1.1.2.zip	43.6 MB
iOS_1.1.2.zip	38.5 MB
photon_darwin_amd64_1.1.2.zip	8.77 MB
photon_linux_amd64_1.1.2.zip	9.16 MB
photon_linux_arm_1.1.2.zip	8.7 MB
photon_windows_amd64_1.1.2.zip	8.85 MB
Source code (zip)	

Photon Network Structure

The main purpose of Photon's technical design construct is to employ a partition layer to realize off-chain micropayments。Below is a chart of its framework:



Photon Smart Contract Key Points

Security Principles

- Neither Party Can Seize a Token from the Main Network
- Regardless of either party providing false/corrupt data, neither party can be damaged
- Regardless of either party providing false/corrupt data, neither party can unfairly benefit
- Neither party on the channel can cause damage to the other party due to non-cooperation or inaction
- Both Channel parties can guarantee the due income regardless of which one provides correct and/or real data

Photon Smart Contract Key Points

Photon Network

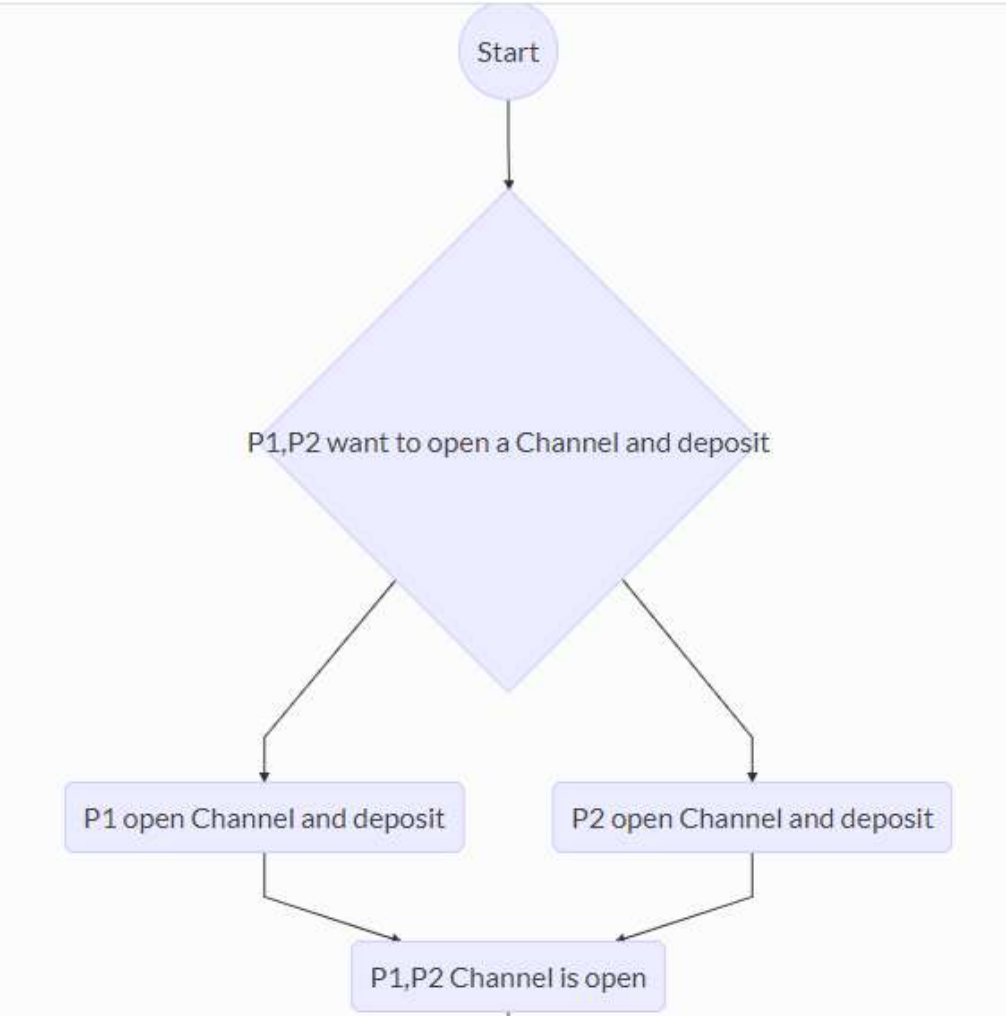
Important Channel States:

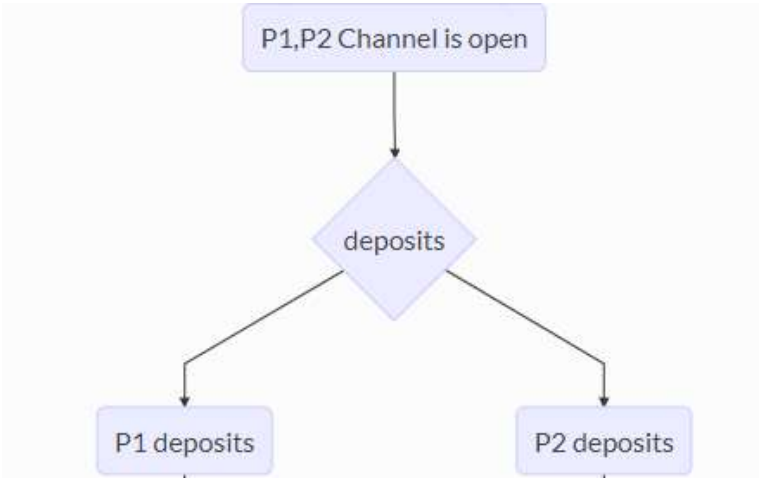
State	StateString	Description
0	inValid	Channels do not exist
1	opened	Channel open status,which can carry out normal offchain transactions
2	closed	The channel is closed, no more transactions can be initiated, but Ongoing transactions can be accepted.
3	settled	The channel is settled which the token will return to the respective accounts on the blockchain, and the channel will be invalid.
4	closing	The participant initiated a request to close the channel, the transactions which is being processed can continue to finish, but the participant cannot initiate new transactions.
5	settling	The participant initiated a settlement request and is processing. Normally, there should be no uncompleted transaction and no new transactions can be initiated. The settling transaction are being submitted to the chain and have not yet been successfully packaged.
6	withdrawing	When the participant receives or sends a `withdraw` request, just at this moment,he receive the transaction request of the other node,the ongoing transaction can only be abandoned immediately.

Photon Smart Contract Key Points

Photon Network

Key Functionality Demo（Channel Setup）：
Channel Setup Combined with a Deposit





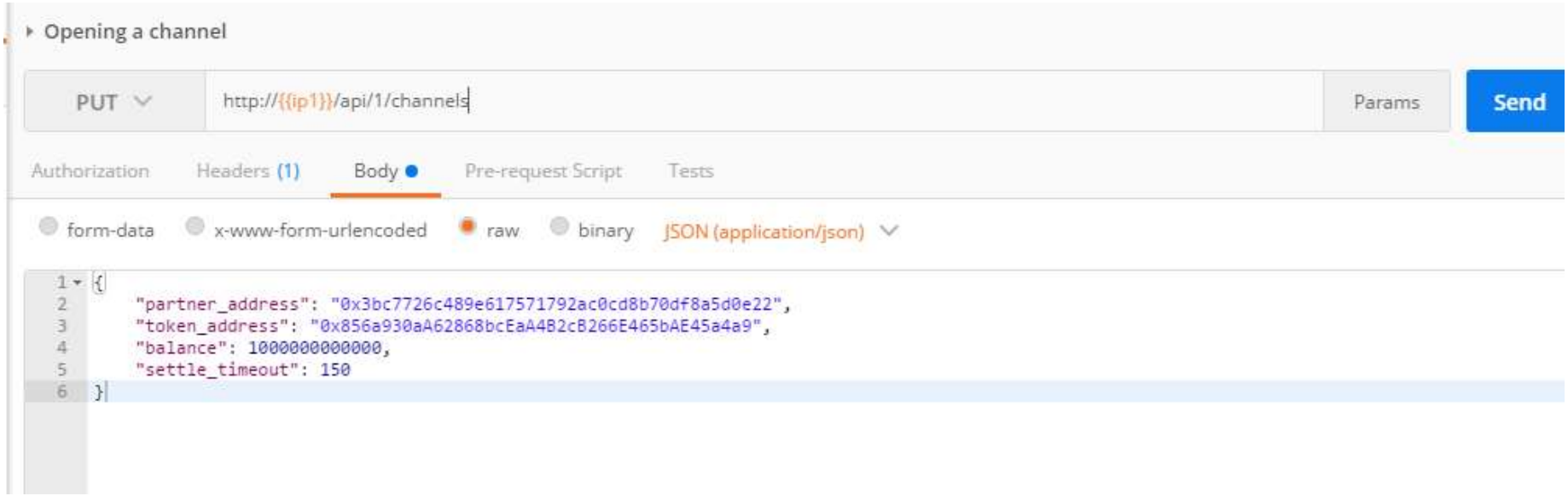
Photon Smart Contract Key Points

```
function deposit(address token, address participant, address partner, uint256 amount,
uint64 settle_timeout) external

event ChannelOpenedAndDeposit(
    address indexed token,
    address participant,
    address partner,
    uint64 settle_timeout,
    uint256 participant1_deposit
);
event ChannelNewDeposit(
    bytes32 indexed channel_identifier,
    address participant,
    uint256 total_deposit
);
event TokenNetworkCreated(address indexed token_address);
```

Photon Smart Contract Key Points

We will demonstrate the deposit function of the photon node. By the way, if the photon nodes are already running in tango, do not run them on Laptops again. Running nodes on different devices will cause database conflicts, so we choose the testnet for DEMO .

PUT /api/1/deposit



Photon Smart Contract Key Points

code:

Channel Setup Combined with a Deposit

```
function deposit(address token, address participant, address partner, uint256 amount,
uint64 settle_timeout)
    external
    {
        depositInternal(token, participant, partner,msg.sender, amount, settle_timeout, true);
    }

function depositInternal(address token, address participant, address partner,address from,
uint256 amount, uint64 settle_timeout, bool need_transfer)
    internal
    {
        bytes32 channel_identifier = getChannelIdentifier(token, participant, partner);
        Channel storage channel = channels[channel_identifier];
        Participant storage participant_state = channel.participants[participant];
        require(amount > 0);
```

Photon Smart Contract Key Points

Photon Network

code:

```
if (channel.state == 1) {
        uint256 total_deposit;

        total_deposit = participant_state.deposit;
        // Update the participant's channel deposit
        total_deposit += amount;
        // make sure not overflow, test equal because of first deposit is equal
        require(total_deposit >= amount);
        participant_state.deposit = total_deposit;

        emit ChannelNewDeposit(channel_identifier, participant, total_deposit);
    }
```

Photon Smart Contract Key Points

Photon Network

code:

```
else if (channel.state == 0) {
        require(participant != 0x0);
        require(partner != 0x0);
        require(participant != partner);
        require(settle_timeout >= 6 && settle_timeout <= 2700000);
        //This token will only be detected when the channel is first created.        if
(!registered_token[token]) {
            validAndUpdateToken(token);
        }
        // Store channel information
        channel.settle_timeout = settle_timeout;
        channel.open_block_number = uint64(block.number);
```

Photon Smart Contract Key Points

Photon Network

code:

```
        // Mark channel as opened
        channel.state = 1;
        participant_state.deposit = amount;
        emit ChannelOpenedAndDeposit(token, participant, partner, settle_timeout,
amount);
    } else {
        //The channel being settled is not allowed to deposit
        revert();
    }
    if (need_transfer) {
        Token token_contract = Token(token);
        // Do the transfer
        require(token_contract.transferFrom(from, address(this), amount));
    }
}
```

Photon Smart Contract Key Points

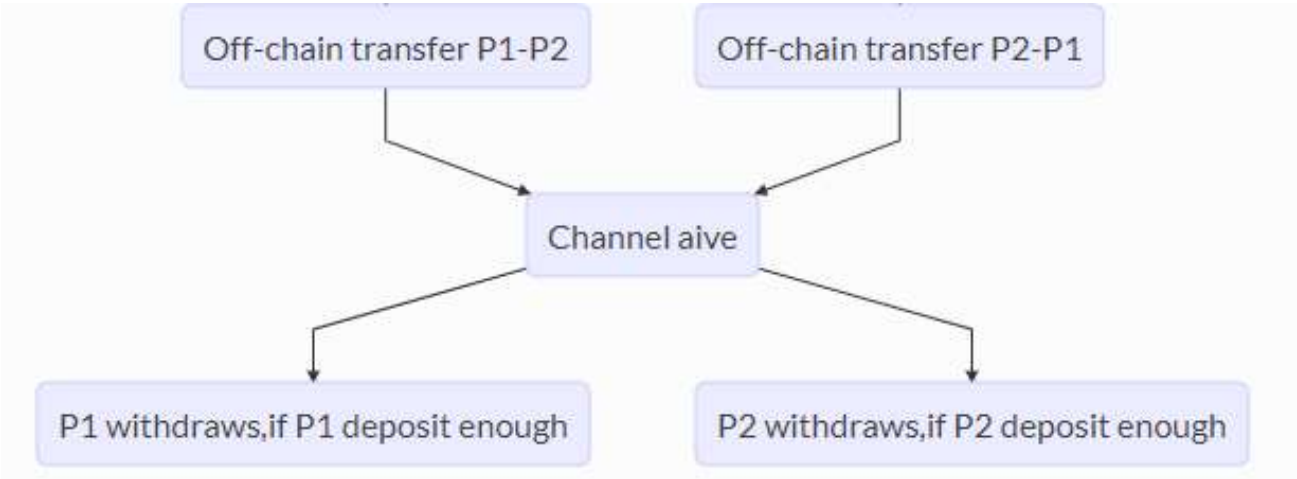
Photon Network

code:

```
        // Mark channel as opened
        channel.state = 1;
        participant_state.deposit = amount;
        emit ChannelOpenedAndDeposit(token, participant, partner, settle_timeout,
amount);
    } else {
        //The channel being settled is not allowed to deposit
        revert();
    }
    if (need_transfer) {
        Token token_contract = Token(token);
        // Do the transfer
        require(token_contract.transferFrom(from, address(this), amount));
    }
}
```

Photon Smart Contract Key Points

Key Functionality Demo:
Not Closing a Channel Withdrawal



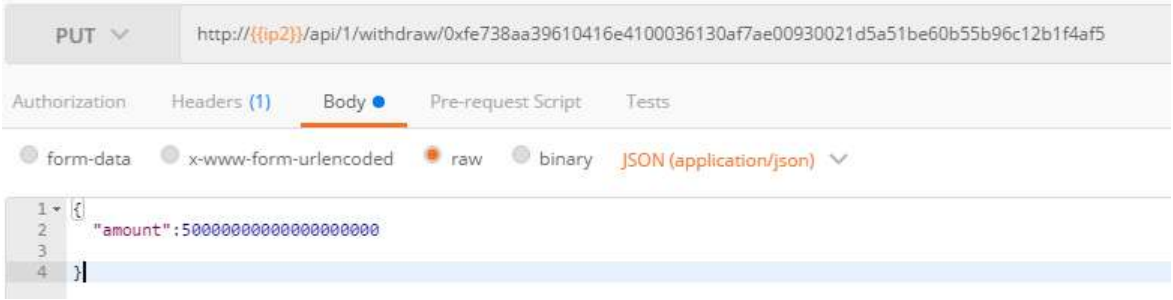
Photon Smart Contract Key Points

```
function withDraw (
        address token,
        address participant,
        address partner,
        uint256 participant_balance,
        uint256 participant_withdraw,
        bytes participant_signature,
        bytes partner_signature)
    public


event ChannelWithdraw(
    bytes32 indexed channel_identifier,
    address participant,
uint256 participant_balance
address  partner,
uint256 partner_balance
);
```

Photon Smart Contract Key Points

Key Functionality:
Not Closing a Channel Withdrawal

PUT /api/1/withdraw/*(channel_identifier)*



Photon Smart Contract Key Points

Photon Network

Code:

```
function withDraw(
        address token,
        address participant,
        address partner,
        uint256 participant_balance,
        uint256 participant_withdraw,
        bytes participant_signature,
        bytes partner_signature
    )
    public
    {
        uint256 total_deposit;
        bytes32 channel_identifier;
        uint256 partner_balance;
        Token token_contract=Token(token);
        channel_identifier = getChannelIdentifier(token,participant, partner);
        Channel storage channel = channels[channel_identifier];
```

Photon Smart Contract Key Points

Photon Network

Code:

```
require(channel.state == 1);
    // Verify that the signatures of both parties are valid
    require(participant == recoverAddressFromWithdrawProof(channel_identifier,
        participant,
        participant_balance,
        participant_withdraw,
        channel.open_block_number,
        participant_signature
    ));
    require(partner == recoverAddressFromWithdrawProof(channel_identifier,
        participant,
        participant_balance,
        participant_withdraw,
        channel.open_block_number,
        partner_signature
    ));
```

Photon Smart Contract Key Points

Photon Network

Code:

```
    Participant storage participant_state = channel.participants[participant];
    Participant storage partner_state = channel.participants[partner];
    //The sum of the provided deposit must be equal to the total available deposit
    total_deposit = participant_state.deposit + partner_state.deposit;
    partner_balance = total_deposit - participant_balance;
    /*
Deduct money before transferring       /*
        Remind the person withdrawing that the amount must not be 0, otherwise it
should  call cooperative settle
    */
    require(participant_withdraw > 0);
    require(participant_withdraw <= participant_balance);
    //Prevent overflow
    require(total_deposit >= participant_balance);
    require(total_deposit >= partner_balance);
```

Photon Smart Contract Key Points

Photon Network

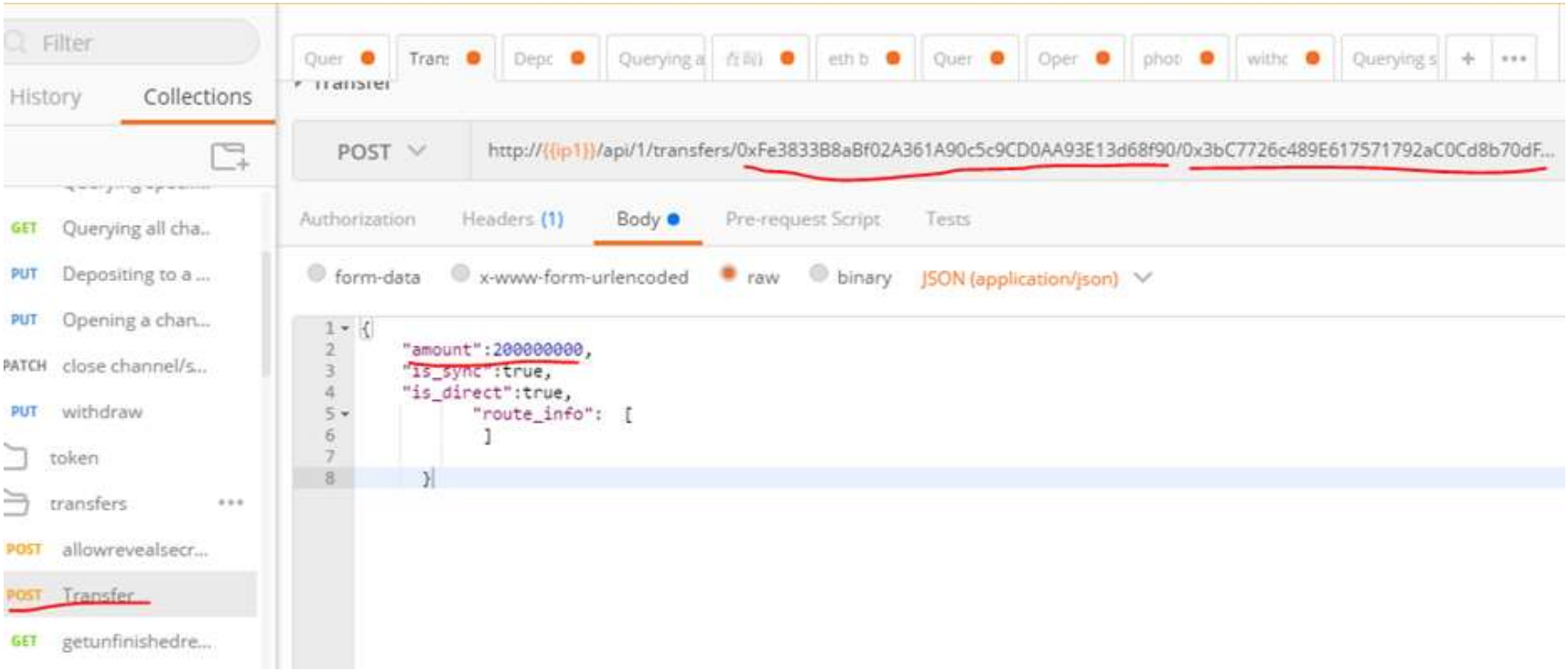
Code:

```
    participant_balance -= participant_withdraw;
    participant_state.deposit = participant_balance;
    partner_state.deposit = partner_balance;

    // It is equivalent to the channel settle again. The old signatures are invalid.
channel.open_block_number = uint64(block.number);
    require(token_contract.transfer(participant, participant_withdraw));

    //channel's status right now
    emit ChannelWithdraw(channel_identifier, participant, participant_balance,
partner, partner_balance);

  }
```

Photon Off-Chain Transfers

Photon Network

Direct Channel Account Transfers:



Photon Off-Chain Transfers

Photon Network

Indirect Channel Account Transfers:

Transfer

POST http://{{ip1}}/api/1/transfers/0xFe3833B8aBf02A361A90c5c9CD0AA93E13d68f90/0xC445a8C326A8fD5a3e250C7dc0EFc566... Params Send

Authorization Headers (1) Body Pre-request Script Tests

form-data x-www-form-urlencoded raw binary JSON (application/json)

```
{
    "amount":100000000,
    "is_sync":true,
    "is_direct":false,
        "route_info":  [
        {
        "path_id": 0,
        "path_hop": 1,
        "fee": 10000,
        "result": [
            "0x3bc7726c489e617571792ac0cd8b70df8a5d0e22",
            "0xc445a8c326a8fd5a3e250c7dc0efc566edcb263b"
        ]
    }
        ]

  }
```

Photon Off-Chain Transfers

Photon Network

Settling and Closing Channels:

close channel/settle channel

PATCH http://{{ip2}}/api/1/channels/0x155254716721e54470a93c2d0ba7e7ffd3a13b19acbaee01b651efd1d1957c22 Params Send

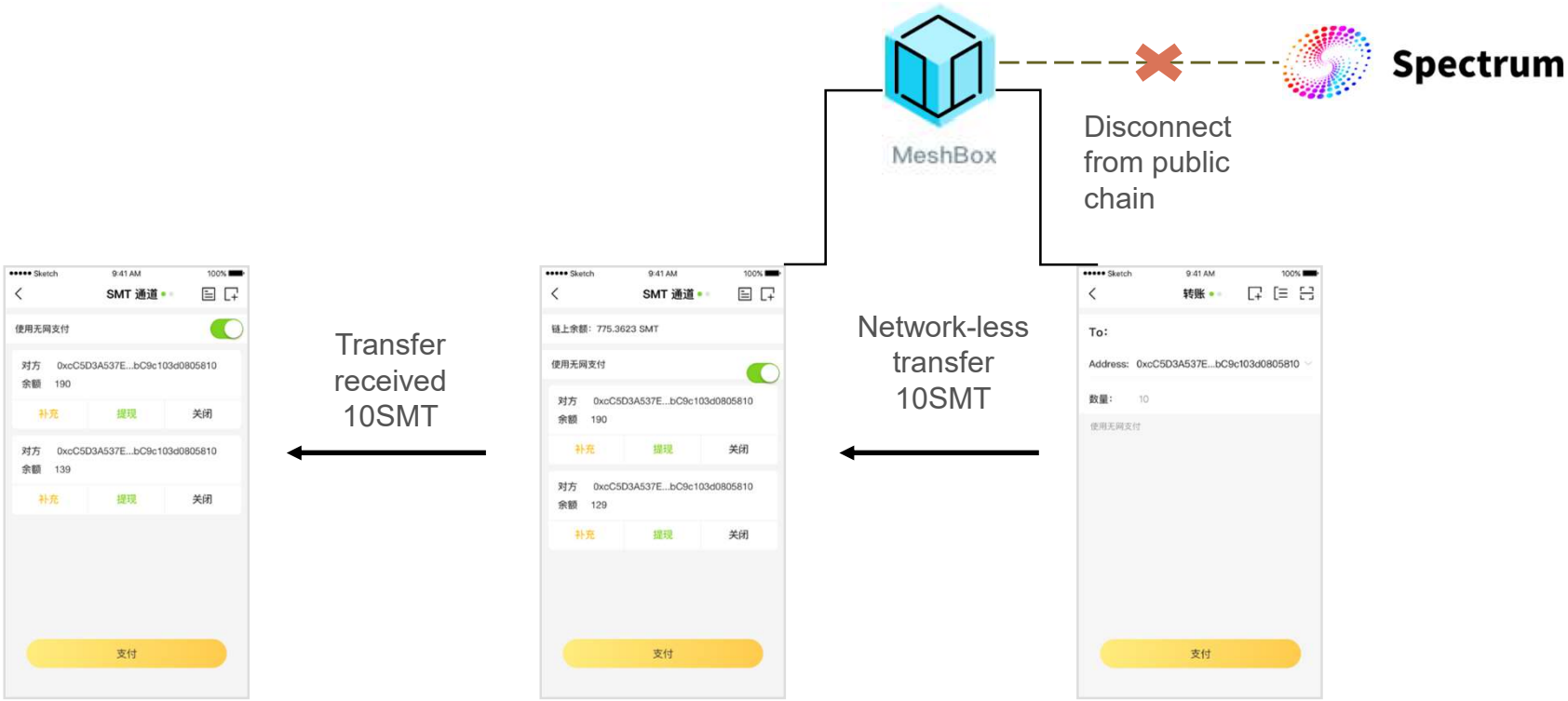
Authorization Headers (1) Body Pre-request Script Tests

form-data x-www-form-urlencoded raw binary JSON (application/json)

```
1 {
2 "state":"closed",
3 "force":false
4
5 }
6
```

Photon Network Special Functionality

- Offline Direct Payments（Play Video）



Other Photon Network Functionality （Roadmap）

Photon Network

(1) Tokenswap

(2) Third-Party Services

(3) Router Services