A ubiquitous, industry agnostic platform for automated, smart contract based, realtime trusted transactions.

Applicant: **OpenCT** Zug, Switzerland

Inventors: **Moustafa Amin -** Cairo, Egypt;

**Mayande Walker** - New York, NY

Abstract

Described is OpenCryptoTrust Token (OpenCT Token)

Described is OpenCryptoTrust Platform (OpenCT).  The OpenCT framework facilitates the creation of attributes and rule sets required for industry specific applications. There are defined metrics with configurable thresholds that can trigger transactions - such as self-executing smart contracts - tailored to the security, regulatory, and legal standards of any industry.

Described is Blockchain as a Transport (BaaT) networking architecture.  BaaT connects geographically dispersed Layer 2 (L2) islands over any available infrastructure, including the public Internet. BaaT securely supports all kinds of network traffic including; Unicast, Multicast, and Broadcast.

Described is Blockchain-Defined Wide Area Networks (BD-WAN) software framework integrating blockchain with Software-Defined WAN (SD-WAN) for a secure, scalable virtualization of WAN transport technologies.

Described is OpenCT platform utilizing the Proof of Trust (PoT) Mining Algorithm as one of two algorithms for distributed low compute power secure blockchain mining for allowing low stakeholders to get the chance to produce blocks over the OpenCT platform and hence get rewarded for their efforts.

Described is OpenCT Token Crowdsale allowing for an increasing linear function to increase the value of tokens over time .

1. Technical Field

Relates to network platform for high volume transactions requiring verifiable transaction tracking.

1. Background

Various industries require access to trusted ledger applications to provide verifiable accounting for their services.  Many industries are highly inefficient, sometimes preventing business flow. Blockchain has been identified as a trusted public ledger platform to allow services to be developed cost effectively to produce new economic optimizations, thereby improving performance and reducing cost of services.  Even Blockchain has its own inherent inefficiencies, requiring massive processor and large amounts of energy to compute a given transaction where the payout for the transaction can be more expensive than the transaction itself. Additionally, Blockchain is limited in the number of transactions per second they can manage, in some cases transactions can take 10 minutes.  For real time high transaction applications, this type of blockchain will not work. Each Market has their own inherent issues.

1. Telecommunications - To transmit data across oceans, telecommunications companies acquire a data pipe based on their expected utilization of data for their business.  Telecommunications customers must purchase more than the peak of their expected usage, causing inefficiencies and over purchasing of bandwidth with long term contracts. This market will leverage the blockchain as a ledger for tracking bandwidth usage at a granular level, allowing for an efficiency in selling parts of a pipeline, instead of the entire pipeline itself.
2. Finance -
   1. Leveraging blockchain for greater speed and efficiently proving the order of electronic trades within a dark pool.
   2. Leveraging blockchain to support the ability to decrypt what under normal conditions are anonymous trading activities within a dark pool (decryption as needed for example during a SEC investigation or regulatory mandated audit of trades).
   3. Lower cost for global remittances.
   4. LBG (Load Balancing Gateway) to support Enterprise Network exchange services - a “router” that can route or exchange between tokens. Ultimately in support of a network that requires a specific utility token for operations but needs to
      1. Build a reserve (based on ANY other token or fiat) to ensure smooth transactional activity.
      2. Provide liquidity for the native token regardless of the form of payment provided by enterprise clients.
3. Artificial Intelligence (AI) OpenCT’s LBG (Load Balancing Gateways) - providing access to both transport services; financial exchange services; and inexpensive compute power from shared compute providers and/or farms and/or mining platforms.
4. Healthcare - leveraging blockchain to provide an immutable ledger of cloud based patient medical records that are owned and managed by patients (or their designated medical representatives/doctors) with the ability to provide secured access on an as needed basis to others. Benefit for patients in terms of responsible ownership of health and benefit to insurance operators who can verify and audit this ledger to make more granular decisions with regard to coverage benefits (and thus lowering costs on a wider scale based on more accurate information).
5. Energy - leveraging blockchain for in immutable ledger that supports multiple overlays of disparate data sources that when combined provide more accurate information (from different divisions within an enterprise; OR different independent enterprises who agree to collaborate) regarding upstream exploration, abstraction, production and midstream storage or transport and downstream refinery and distribution.
6. Supply Chain - leveraging blockchain to create efficiencies in the ordering, manufacturing and logistics processes of large scale global entities.
7. Real Estate - leveraging blockchain in support of A) Tracking of land title rights; B) tokenization (and greater liquidity) of real estate assets.
8. Intellectual Property - leveraging blockchain to support tracking, distribution, and liquidity (via tokenization) of IP.
9. Cryptocurrency - Open CT Proof of Trust (PoT) can provide variable transaction requirement reducing the processor and energy demands of encrypting and decrypting blockchain and cryptocurrency transactions without losing security or blockchain based tracking.

# Claims:

1. OpenCT Token

A method performed at a computer system that includes a CPU, memory, a hard drive, and a network, the computer system configured to communicate via the network with a centrally managed distributed blockchain computer system that includes multiple computing nodes, each computing node storing a copy, or a portion thereof, of the blockchain of the centrally managed distributed blockchain computer system, the method comprising:

storing at least one ordered list of a plurality of data transaction requests that each include header data for a transaction, a type identifier and a quantity value; and

storing a plurality of digital wallets that are respectively associated with different client entities, each of the plurality of digital wallets respectively linked to at least one corresponding private cryptographic key and at least one identifier that has been generated based on the at least one private cryptographic key;

receiving, via the central computing device and from different remote computing devices, electronic data messages that each include data transaction requests;

adding a received first data transaction request, which is associated with a first digital wallet, to the at least one ordered list;

receiving a second data transaction request, which is associated with a second digital wallet;

identifying a match between at least the stored first data transaction request and the received second data transaction request;

generating a first hash identifier based on data included in the first digital wallet;

generating a second hash identifier based on data included in the second digital wallet;

generating a first blockchain transaction that is based on the first hash identifier and the second data transaction request and submitting, to at least one node of the centrally managed distributed blockchain computing system, the generated first blockchain transaction for inclusion into the blockchain of the centrally managed distributed blockchain computing system;

generating a second blockchain transaction that is based on the second hash identifier and the first data transaction request and submitting, to at least one node of the centrally managed distributed blockchain computing system, the generated second blockchain transaction for inclusion into the blockchain of the centrally managed distributed blockchain computing system;

monitoring the blockchain to verify that the first blockchain transaction and the second blockchain transaction have been included into the blockchain; and

based on verification that the that the first blockchain transaction and the second blockchain transaction have been included into the blockchain, updating at least one record of a database that is external to the centrally managed distributed blockchain computing system.

* 1. Proof of Trust (PoT)

A mathematical equation utilizing one or more of; The Number of Tokens a miner has in their wallet, the Proof of Stake (POS), Proof of Duration (POD), Risk Value, QOS, Encryption, Voting Activity, Security Level, Commitment, the OpenCT Risk (OCTR) of the transaction type, and the Consensus ranking of the Miner.

* 1. OpenCT Risk (OCTR) per computing node in the network

monitoring the crypto trust rating of a computing node prevents malicious break-ins of nodes

* 1. OpenCT Token Crowdsale  
     A method for selling OpenCT tokens to investors.
  2. OpenCT Marketplace  
     A method for buying and selling tokens to users of the OpenCT platform

A method for buying and selling network access to users of the OpenCT Platform

* 1. OpenCT Platform

A centrally managed distributed blockchain computing system used for;

control plane, instructions, reporting, and auditing in “real time”.

using Proof of Trust (PoT)

using OpenCT Risk (OCTR)

using OpenCT Crowdsale

using OpenCT Marketplace

1. Blockchain as a Transport (BaaT)

A centrally managed distributed blockchain computing system ledger as a means of disseminating Layer 2 networking information across a routed network using the OpenCT Platform for managing assets.

An advanced Layer2 VPN solution using the public Internet for traffic.

Built to operate in a scalable multipoint fashion. Its signaling is done via the blockchain

Multicast and broadcast traffic is handled via the head-end replication

1. Blockchain-Defined Wide Area Networks (BD-WAN)

Smart contracts associated with the build up and tear down of network circuits in support of bandwidth on demand using the OpenCT Platform for network transactions.

A controller that is northbound controlled via blockchain.

Nodes installed to which the local WAN resources are directly connected via a network

Using the OpenCT platform.

using secure communications between the controller and the centrally managed distributed computing systems.

# Logical Flow

1. DESCRIPTION: OpenCT Token

Blockchain technologies provide valuable trusted technical components that allow for a transaction to be validated by the blockchain network of servers and miners. Current Blockchain mining is designed to become more complicated over time to ensure security against faster and more powerful computers cannot break the security encryption during a mining operation.  This in turn requires a combination of increased computing power and energy on the part of the miner. For slow transactions where miners are rewarded for these transactions, this works just fine. For high volume, low value transactions, this type of encryption/decryption becomes a burden on the part of the application.

Proof of Trust (PoT) allows a Miner Trust Value to be created that allows a transaction to use lesser encryption, thereby reducing compute and energy requirements on the part of the Miner to perform a transaction.  This further allows for larger volume of transactions to be spread out requiring lower compute power and energy for high volume transactional blockchain applications.

The Blockchain Mining Algorithm plays a significant role in what can be done with the model including the mining activities and rewards to a large decentralized community. PoD (Proof of Duration) which when used in combination with PoS (Proof of Stake) or DPOS (Delegated Proof of Stake) provides for a more democratic approach to mining and consensus. The OCT Token utilizes this PoD algorithm to address the token mining speed and security required for managing large volumes of transactions onto the blockchain. A block production rate that can be exceptionally fast, upwards of 100,000 TPS (Transactions Per Second).

1. Proof of Trust (PoT)
   1. A mathematical equation utilizing one or more of; The Number of Tokens a miner has in their wallet, the Time Duration a miner has held those tokens, the Risk Value of the transaction type, and the Consensus ranking of the Miner.  The separation of High, Medium and Low is an arbitrary assignment, meaning there can be an infinite number of rankings and weightings for each of the defined segments. Examples are shown only for discussion purposes, not for actual implementation purposes.
      1. PoS (Proof of Stake) or DPOS (Delegated Proof of Stake)  
         Number of Tokens owned by the miner/node
         1. High - $10,001 to unlimited worth of OCT Tokens
         2. Medium - $101 to $10,000 worth of OCT Tokens
         3. Low - $.01 to $100 worth of OCT Tokens
      2. Proof of Duration (PoD):  
         How long a node has been operating with trust on the network
         1. High - Greater than 1 year
         2. Medium - 1 week to 1 year
         3. Low - 0 minutes to 1 week
      3. Risk Value:
         1. High - Currency, Legal Contracts, Government Laws, Real Estate
         2. Medium - Digital Records (Per Usage Billing For Telecommunications)
         3. Low - Social Media Messages, SteamIt, Telco Signaling Apps
      4. Reputation: (Consensus Duration: (QoS (Response))  
         How many times the miner has transacted a consensus transaction on the blockchain.  Used to show QoS.
         1. High - 100,001 and Up
         2. Medium - 1,001 to 100,000
         3. Low - None to 1,000
      5. Encryption Complexity:  
         Plays into the compute power available at the client end, and the time/power necessary to encrypt/decrypt a transaction.
         1. High - AES-256
         2. Medium - AES-192
         3. Low - AES-128
      6. Voting Activities:  
         Participation within the blockchain. On screen activities.
         1. High: Always Active
         2. Medium: Active
         3. Low: Not Active
      7. Security Level:  
         Concerns the algorithm used to encrypt/decrypt transactions and the ability of the client device to handle the calculation. Both miner and blockchain need to agree to perform these transactions.
         1. Top secret: Highest degree of protection for information that is paramount in national defense matters and whose unauthorized disclosure may cause extremely grave danger or damage to the nation.
         2. Secret: Unauthorized disclosure of which may result in serious damage or danger.
         3. Confidential: Unauthorized disclosure of which may undermine operations.
         4. Restricted: Unauthorized disclosure of which is undesirable.
         5. None: Not secret, Public
      8. Commitment
         1. High
         2. Medium
         3. Low
   2. OpenCT Rating (OCTR)   
      Miners are allowed to mine for specific types of transactions based on their OpenCT Rating. Miners are rewarded differentially based on the Risk Value of the transaction, and the number of transactions they are allowed to mine based on their OpenCT Rating.
2. OpenCT Token Crowdsale

Open CT will undergo all required steps for a token crowdsale funding the Open CT platform as per SEC guidelines.

Until the Open CT platform is fully developed, the Ethereum blockchain will be leveraged for the creation of the OCT token and this will also be the platform of choice for all of the crowd-sale activities.

Initially the OCT tokens will be launched as ERC-20 tokens over the Ethereum platform via proper smart contracts: a smart contract for the pre-token crowdsale and another one for the token crowdsale. The token designation at these stages will be ‘OCTb’ or OCT before-platform.

There will be a finite maximum number of OCTb tokens of 250,000,000 (250M) tokens.

[Figure 22] Token Distribution

A pre-token crowdsale and a token crowd sale will take place in sequence.

Both pre-token crowdsale and token crowdsale combined will represent 50% of the maximum supply of tokens.

All potential private investors, pre-token crowdsale investors, and token crowdsale investors will be able to acquire OCTb via any available payment method. The available crypto payment methods will beETH and BTC,and possibly others. The traditional FIAT payment methods will be debit/credit cards, PayPal, and wire transfer.

The OCTb tokens will be swapped to OCT tokens after the development of the OpenCT platform. With the OpenCT platform fully functioning, the OCTb tokens will be swapped to OCT tokens in a 1:1 ratio. Details about the special wallet for the OCT token as well as the swapping mechanism will be published in the near future.

The smart contract that receives the crypto funds during the pre-token crowdsale and token crowdsale are multi-signature wallets requiring the signatures of more than one OpenCT board executive for any transfer or cash out operations.

Tokens purchased during the pre-token crowdsale and token crowdsale will be distributed to the investors in 1-2 week periods after the conclusion of the token crowdsale.

Unsold tokens during the pre-token crowdsale and the token crowdsale will be burned out to protect the integrity of the whole project.

Pre-Token Crowdsale

During the pre-token crowdsale, 10% of the total maximum supply-- **25,000,000 (25M) OCTb**tokens-- will be available for purchase directly or via any private deal. The OCTb token price will follow an increasing step function as follows:

For the first month of the pre-token crowdsale; the token price will be at **US$0.75** (its equivalent in ETH).

For each consecutive month, the price of token will increase by **US$0.0375**, i.e. **US$0.7875** for the second month, **US$0.825** for the third month, **US$0.8625** for the fourth month and **US$0.9** for the fifth month.

For private deals that constitute more than 15% of the pre-token crowdsale, token share (more than 3,750,000 OCTb tokens), special bonuses will apply but the tokens will be held in the smart contract for periods that depend on the investment for the sole reason of protecting public investors’ investments.

For any private deal that constitutes between 15%-20% of the pre-token crowdsale token share (between 3,750,000 and 5,000,000 OCTb tokens), the token price will get a 20% discount from its original pre-token crowdsale price (US$0.6 equivalent in ETH), but the sold tokens for that private deal will be locked in a smart contract and will be released by 50% every 12months over a 2-year period.

For any private deal that constitutes more than 20% of the pre-token crowdsale token share (more than 5,000,000 OCTb tokens), the token price will get a 25% discount from its original pre-token crowdsale price (US$ 0.5625 equivalent in ETH) but the sold tokens will be locked in a smart contract and will be released by 50% every 18months over a 3-year period.

Token Crowdsale

During the token crowdsale, 40% of the total maximum supply-- **100,000,000 (100M) OCTb** tokens -- will be available for purchase.

During the course of the token crowdsale, instead of following a bonus structure common in the crypto world, the OCTb token price will follow an increasing linear function where:

* The price of the first token will be equivalent to the starting price of the pre-token crowdsale (**US$ 0.75**) multiplied by a 25% increase factor (**US$ 0.9375** equivalent in ETH); and
* The price of the last token will be equivalent to the starting price of the pre-token crowdsale (US$ 0.75) multiplied by a 75% increase factor (**US$ 1.3125** equivalent in ETH).

In order to craft the linear equation; the inputs are stated as follows:

* The amount of OCTb tokens available to be sold during the token crowdsale is 100,000,000
* In the examples and use cases below, we will make our calculations in US$. It is worth noting that the real implementation will be based on ETH, according to its exchange rate against the US$.
* F, the price of the first ever OCTb token to be offered during the token crowdsale is equivalent to $0.9375.
* L, the price of the last ever OCTb token to be offered during the token crowdsale is equivalent to $1.3125.
* So for any OCTb token (t) that comes in between the first and the last tokens, its price is determined by a linear function called P(t):

**P(t) = 0.9375 + \*t**

Where the ‘0.375’ value is the difference between the final and initial prices in US$:

[Figure 23]

As an example, imagine an investor who holds a certain amount of US$ (U) and he wants to invest that amount by participating in the token crowdsale and purchasing (B)tokens. Further imagine that at the same time this investor wants to participate and buy tokens, there is actually (A) tokens that have been sold for other investors.

As the price of the OCTb tokens during the token crowdsale is determined by a linear function, so the initial price for the tokens that this investor will pay is just on the P(A) mark and the final price he’ll get a quote for is P(A+B)

[Figure 24]

In order to identify how many tokens this investor will be able to acquire with the U amount of US$, we have to solve the below equation (finding the area under the curve highlighted in yellow);

**) dt**

Solving this integral function gives us:

**U = (0.9375)\*(B) + \* (+2AB)**

Making a few assumptions for the variables in this equation in order to give an example:

U = 100 US$ and A = 1,000,000 Tokens

So:

100 = (0.9375)\*(B) + \* (+2,000,000B)

Putting it in the normal 2nd degree equation format:

0.000000001875+ 0.94125 B – 100 = 0

Then:

B = 106.24167737364769 Tokens

In order to calculate the full amount in US$ that will be raised during the tokencrowdsale, use A=0 and B = 100,000,000.

As:

**U = (0.9375)\*(B) + \* (+2AB)**

Then:

U = (0.9375)\*100,000,000 + \* () = US$ 112,500,000

The minimum cap for both the token pre-crowdsale and crowdsale is set at the **US$ 15M** mark while the maximum cap is only limited by the number of available tokens during the token crowdsaleas well as the duration of the token crowdsale.

If that minimum cap condition is not met, the smart contract will reverse itself automatically and the money (crypto or traditional FIAT) will be paid back to the investors (from both phases: pre-crowdsale and crowdsale)

The OCTb token will be available for trading 4 weeks after the conclusion of the token crowdsale at the selected exchanges. The selected exchanges will be shared with the OpenCT community in a timely manner.

**[Figure 25]: The OCT rewarding system**

Miner Reward System

The OpenCT platform has a unique rewarding structure for its users.

To understand the rewarding structure, we must first define the users of the platform.

The users are miners (block producers) who download the platform, keep it running in order to verify the broadcasted transactions and pack them into proper blocks to be hard coded (glued) to the blockchain.

Anyone can participate in the OpenCT operation as a user. There are two ways to do that but both require holding some amount of tokens in their wallet:

* **OCTb/OCT Token large-amount holders**: These holders either participated in the pre-token crowdsale and/or token crowdsale (OCTb token), bought tokens after the conclusion of the token crowdsale (OCTb token), or bought tokens after the launch of the OpenCT platform (OCT token). These large-amount token holders will be selected and nominated via the PoS algorithm in proportion to their actual holdings, to become block producers and hence to be rewarded accordingly.
* **OCT Token low-amount holders**: These holders bought OCT tokens after the launch of the OpenCT platform. These low-amount holders will be selected and nominated via the PoD algorithm in proportion to the longest duration they’ve kept at least one (1) OCT token in their wallet, to become block producers and hence to be rewarded accordingly.

The rewarding structure of the OpenCT platform is one of a kind. It’s structured according to a creative mathematical constant ‘e’ and the [Bernoulli compound interest formula](https://en.wikipedia.org/wiki/E_(mathematical_constant)).

The total number of tokens used to reward the block producers represents 15% -- 37,500,000 tokens -- of the maximum supply of tokens:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Year-1 | Year-2 | Year-3 | Year-4 | Year-5 | Total |
| Start number of Reward Tokens per Year | 7,000,000 | 6,500,000 | 6,000,000 | 5,500,000 | 5,000,000 | 30,000,000 |
| Annual Profit (%) | 30 | 26 | 22 | 16 | 12 |  |
| Number of Reward Tokens - Simple Profit | 9,100,000 | 8,190,000 | 7,320,000 | 6,380,000 | 5,600,000 | 36,590,000 |
| Number of Reward Tokens – Compound Interest - Jacob Bernoulli | 9,449,012 | 8,430,046 | 7,476,460 | 6,454,310 | 5,637,484 | **37,447,312** |
| Number of Reward Tokens - Compound Interest - Quarterly (n=4) | 9,348,284 | 8,362,031 | 7,432,948 | 6,434,222 | 5,627,544 | 37,205,029 |
| Number of Reward Tokens - Compound Interest - Weekly (n=52) | 9,440,869 | 8,424,586 | 7,472,992 | 6,452,724 | 5,636,705 | 37,427,876 |
| Number of Reward Tokens - Compound Interest - Daily (n=365.25) | 9,447,848 | 8,429,266 | 7,475,965 | 6,454,084 | 5,637,373 | 37,444,536 |

The structure starts by assigning a fixed number of reward tokens per year over a five (5) year period. This number decreases year-over-year.

A fixed annual profit is chosen for each year, again in a decreasing fashion, in a way to attract more adopters (and hence block producers) at the start of the OpenCT platform operation while attracting more users over a five-year period.

Solving Bernoulli’s formula for the first year, given our inputs:

* Initial Value for the first year = 7,000,000 tokens
* Annual interest (R) for the first year = 30%, so R = 0.3
* The number of years (t) here is 1

The original equation is:

Total value = Initial Value \*

So, the maximum number of tokens that can be offered as rewards for the first year will be equal to:

7,000,000 \* = 9,449,012 Tokens.

The same calculation applies to the second, third, fourth and fifth years.

The sum of all maximum compounded number of tokens over the 5-year period is:

**37,447,312**

So it is clear that according to the Bernoulli formula with the mathematical constant ‘e’ that the maximum number of reward tokens offered over the 5-year period will never exceed 37,500,000 tokens (the available number of reward tokens according to the token distribution structure).

This way we can insure that the actual rewarding figures will never exceed what we reserved for the rewarding structure.

Taking the third year as an example, we will compound the composite interest every week, so:

* Initial Value for the third year = 6,000,000 Tokens
* Annual interest (R) for the third year = 22%, then R = 0.22
* n = 52

The equation for the number of tokens for the third year after the weekly compounding is:

Initial Value \*

Substituting:

6,000,000 \* = 7,472,992 Tokens.

As the fixed number of assigned reward tokens decreases year over year, so does the annual profit. That is balanced by compounding more frequently year over year.

1. OpenCT Marketplace
   1. The OpenCT Marketplace allows users of the system to purchase items including tokens, network bandwidth, and digital assets.
   2. [Figure 28] OpenCT Marketplace - Bandwidth
      1. A Request is made of the system to send digital assets through a network. The OpenCT Marketplace reviews the assets to be sent through the network, determines which network has the appropriate bandwidth and price for the package, and send the package to the destination using the right Telco and Telco client / network.
   3. OpenCT Marketplace - Tokens
      1. A Centrally Managed Token system for managing the OpenCT Token.
      2. Manages Initial value of the OpenCT Token using OpenCT Crowd sale to establish value
      3. Manages access to the tokens for buyers and sellers.
      4. Manages the exchange of tokens for use in the network.
2. OpenCT Platform (Blockchain)

* The blockchain system used for; control plane, instructions, reporting, and auditing in “real time”.
* [Figure 14] Blockchain Propagation
  + No need for network propagation - the blockchain maintains a continuously updated state for the network.
  + BD-WAN Controller Cluster tracks the health status of all nodes A through M in the network and propogates routing tables to all nodes.
    - Blockchain: All nodes (A through M) in the blockchain receive regular routing information updates very quickly, currently clocked at 250 ms. This rate will change based on the needs and capabilities of the network. The Blockchain related processing time is the total propagation speed of node update is based on the mesh of the network and propagation. Blockchain keeps only networking propagation information, not the data itself.
  + When transmitting information from Source “1” to Destination “2”, a network route will be sent to nodes A-M from the BD WAN Controller Cluster. Controlled nodes, which already has the optimal route determined.
  + Use Case: **Inbounds Success** - Nodes in the blockchain routing are processing updates properly.
  + Use Case: **Node failure**: A message is sent to the BD-WAN Controller Cluster to have it update the routing table and put the new routing table in the next update for the route. When that node returns to full use, it will be put back into the routing table.
  + The processing at the node includes decrypting the routing table and is near zero in time.
  + Useful for streaming applications where network interruptions cause a breakdown in quality of service.
    - Improvement in delivery QOS for streaming
    - TCP/IP and UDP (etc…) still necessary, but TCP doesn’t need to be the only technology.
* [Figure 15] Asset Creation and Transactions
  + [Figure 15 (a)] Assets can be created from any node in the blockchain. Create a new asset named ‘asset1’ with 1000 units, each of which can be subdivided into 100 parts and send it to self.
  + [Figure 15 (b)] Verify that the new asset named ‘asset1’ is created and listed successfully.
  + [Figure 15 (c)] Inspecting it from another node attached to the same blockchain.
  + [Figure 15 (d)] Checking the balance of the created asset on the originating node, it is 1000 (the full balance).
  + [Figure 15 (e)] Checking the balance of the created asset on the other node, it should be 0 (no output meaning no balance has ever been transferred to this node yet).
  + [Figure 15 (f)] Sending 100 units of the created asset from the originating node to the other node.
  + [Figure 15 (g)] Checking the new balance on the originating node (it is now be 900 after deducting the 100 units just sent out).
  + [Figure 15 (h)] Checking the new balance of asset from the other ‘receiving’ node (it is the 100 units just received).
* [Figure 16] Data Storage and Retrieval
  + [Figure 16 (a)] Create a stream on a source node.
  + [Figure 16 (b)] Publish information on the created stream (a key and some hexadecimal data). Note that the chosen hexadecimal data ‘637573746f6d65722031353520766e6964203130343030’ is not random. It has some meaning. This demonstrates the entry of the hexadecimal data.
  + [Figure 16 (c)] Inspecting the created stream from another node attached to the same blockchain, note the number of keys (1) in stream100.
  + [Figure 16 (d)] Digging deeper and fetching more detailed information regarding the keys inside stream100, you can see that key1555 contains ‘1’ item (the published hexadecimal data):
  + [Figure 16 (e)] Publishing other hexadecimal data item from the other node.
  + [Figure 16 (f)] ‘637573746f6d6572203135353520766e6964203132353030’ on the same stream & key pair (stream100, key1555).
  + [Figure 16 (g)] Inspecting the stream from the source node.
  + [Figure 16 (h)] Digging deep into stream100 and we see its keys (key1555) as well as the key contents (2 items).These are the two hexadecimal data items published.
* [Figure 17] Hybrid blockchain
  + Both public and private
    - Public is used for documents / money / digital assets
    - Private is used for network propagation
  + Block producers handle all blockchain blocks
* [Figure 18] Blockchain growth management -
  + Blockchain node B (and all nodes in the blockchain) uses a combination of removal, compression, and archiving to manage the blockchain stack size on the node.
  + [Fig 18] Removal / compression / archiving
    - Removal By Expiration Date
      * The system will reduce the blockchain stack based on the type of data stored in the blockchain removing data with an expired expiration date.
      * Example:
        + Network routing information may not be useful within 1 second of it’s propagation,
        + Legal documents could have a 5 year expiration date (end of contract)
        + Money has no expiration date (exists forever).
      * Nodes in the blockchain don’t carry the entire blockchain Ledger
      * Lightweight version of a wallet only carries the header
    - Compression
      * Blockchain entries are compressed.
        + Compressed ledgers are compared as if they were standard blockchain ledgers
      * Metadata is the only thing saved in the blockchain, and each metadata represents section(s) of the chain.
        + Absolute finality - there is no period of uncertainty in the compression blockchain. Once the chain is built, there is no period of negotiation. Convergence is final, doesn’t require contesting, or back and forth of information. We send all routing information to the nodes simultaneously.
    - Archiving
      * Blockchain ledgers are archived off the node to enable the node to continue to function when they exceed a certain size limit.
      * Nodes that carry the full uncompressed chain are archived.
    - Compromised nodes are validated against
      * Routing data is flushed, revalidated, and updated once again.
      * In case of compromised data, the node is flushed, and treated as a new node, built up from scratch, and comes on line as if it were just added to the network.
      * Node gets put on a watch list to track against Proof of Trust.
    - Features/Benefits
      * Efficiencies:
        + Much more transactional activity can be captured / acted on
        + Much less maintenance
        + Uses less network bandwidth

Re-transmission of packets (aka TCP/IP) not necessary

TCP/IP used to guarantee payloads

* + - * + Uses less energy
        + Uses less computational power
        + Faster streaming media using no TCP/IP for data transmission allowing exponential growth in media streaming clients. Broadcast routing tables allow streaming media to be delivered to the client including any node loss along the routing path due to the inability of a human to perceive a routing table update drop in audio or video.
        + More reliable than TCP/IP Routing for transmission of data.
        + Speed and efficiency of data transport for internet access
    - Convergence
      * Need to flood an environment with news about a bad route
        + Once a bad route appears, the entire network must know that a route is no longer valid.
        + Once a route is found to be invalid, what is the next valid route?
      * These are eliminated with Open CT,
        + Any route found to be invalid, immediately updates the entire network with the new route
        + No local calculation required
    - [Figure 19] TCP/IP and OpenCT Blockchain operating together
      * Logic of a packet in BaaT / BD-WAN network
      * BD-WAN Device broadcasts routing data to OpenCT Blockchain routing nodes every N ms (currently every 250 ms). Nodes A-G and Source/Destination 1 & 2 receive routing data from BD-WAN.
      * Header information and payload are published from point A to point G and Source/Destination 1&2 using the OpenCT BaaT network
        + Payload in BaaT Verified by Baat using Header information

If BaaT verification fails, payload is requested again

* + - * + TCP/IP used to verify that the whole package arrived and is complete to fit in with TCP/IP networks

If TCP/IP verification fails, payload is requested again

* + - * [Figure 27] BD-WAN Logical Diagram
        + OpenCT Blockchain BD-WAN Controller
* Routing protocol vs. Propagation Protocol
  + Routing protocol is a subset of Open CT propagation protocol
  + More efficient routing protocol
    - Greater stability
    - Steady state
  + Components of failure
    - Failure Detection (standard)
    - Failure Propagation (standard)
    - New Path Calculation (unique)
      * Time reduction from minutes to 250 ms (near real time)
* (Close to EOS)
  + UTXO - Proof that someone has shared an amount of currency
  + Open CT Blockchain is concerned with the metadata that is stored and that it is retrievable, not the transaction of a currency
  + Open CT is more like EOS, to execute smart contracts
  + (IPFS)
  + Storing the metadata about a network transfer rather than the data that was transferred.
  + Typical Metadata
    - Source
    - Destination (for addresses
    - Payload type / traffic type
    - VLAN ID
    - QOS
    - MPLS Header fields
    - Open FLOW Headers

How blockchain and distributed ledger are used in support of:

* **Routing of Data Packets** - Mechanism for how nodes receive routing of data packet information
* **Smart Contracts** - scaling up and scaling down of a circuit and tying that to a smart contract
  + Real Time billing
  + Bandwidth on demand
  + Immutable Record
* **Data Transport Layer Functions**
  + Extension of VXLAN by leveraging blockchain/distributed ledger to extend the reach of VXLAN
  + A necessary component for data transport layer
    - Handles
      * Routing
      * Data transport services
        + [Figure 20] Compare BaaT Protocol to other well known data transport protocols including TCP (Mayande to fill out chart)
        + How do we stack up against Transport Layer?
* Smart contract component - monitoring the level of data, held within the blockchain, how we achieve bandwidth on demand
* [Figure 21] Governance
  + Layer 2 Encrypted BaaT Encapsulation Data Flow in support of VXLAN
  + VTEP - VXLAN (Virtual Extensible Local Area Network) Tunnel End Point
  + Phase 1 Original Layer 2 Data Packet -pre Encryption and VTEP - VXLAN (Virtual Extensible Local Area Network) Tunnel End Point.
    - This is the traditional layer 2 frame that would traverse a LAN environment.
  + Phase 2 VXLAN encapsulated to become “layer 3 capable”
    - This is a standard layer 3 packet leveraging VXLAN protocol. It includes the creation of a VTEP (VXLAN Tunnel End Point). NOTE: Not Internet routable (limited to data center or cloud via 1 network hop)
  + Phase 3
    - In this stage there are 3 things that are happening:
      * Blockchain Control Plane Abstraction - the VXLAN packet becomes abstracted into two separate packets - one for control plane, the other for data plan.
      * BaaT Encryption - both packets become AES-256 encrypted.
      * BaaT Encapsulation - both packets become the basis for a new layer 3 packet (now Internet routable). The data plane packet (all “envelope” information has been stripped - all destination MAC, Vlan, Internal IP and port information) gets routed to public IP of destination. All control plane data (“envelope”) and MAC to VTEP mappings are BaaT encapsulated and routed over blockchain to the destination node.
  + Phase 4
    - The destination node reassembles the two packets into a single VXLAN encapsulated packet (identical to packet in Phase 2).
  + Phase 5
    - The VXLAN packet gets de-encapsulated into a standard layer 2 frame.
  + Node State Advertisements (NSA) Link State Advertisements (Gossip Protocol)
    - Supports the ability to eliminate the chatter that is necessary to determine consensus
    - Sustain relevance to how the network should be organized
    - We can hash how that node would react when given an option for decisions
    - We can determine what any node would vote on based on what that node knows about the NSA

1. DESCRIPTION: Blockchain as a Transport (BaaT)

BaaT is useful for any critical high-frequency trading application as described above.  These applications require many events and transactions to be recorded over the blockchain while at the same time ensuring maximum stability, scalability, security, and requiring the fastest convergence time.

BaaT solves many of the disadvantages of other overlays by integrating blockchain with Virtual Extensible LAN (VXLAN). VXLAN was originally drafted as an overlay technology that can work without a control plane. It has proven to be an overlay of choice, but its scope is normally limited to a single data center or cloud.

BaaT greatly enhances the operation of VXLAN by adding a control plane component to it, and extending the VXLAN working domain beyond the boundary of a local data center or even a public cloud.

BaaT operation across the public Internet is appealing as a viable WAN option for many network operators such as enterprises, service providers, and telcos in front of conventional, expensive WAN options such as dedicated links, MPLS, or Virtual Private Networks (VPNs).

[Figure 1] BaaT achieves control plane operation via blockchain.

In this mode, the VXLAN Tunnel Endpoints (VTEPs) are also nodes of a public or private blockchain that can span the public Internet.

[Figure 2] The local MAC learning technique is the same as with any other VXLAN operation: The VTEPs learn the local MAC addresses via their local ports, as shown: BaaT Initial State, and then the addresses are advertised/published as reachable through their VTEP IPs over the blockchain using transactions that are packed into proper blocks.

Steps to publish a stream of hexadecimal data over the blockchain:

1. VTEP Converts Alphanumeric Text to Hexadecimal Text
2. VTEP publishes the Hexadecimal Text over the blockchain
3. The other recipients VTEPs retrieve the Hexadecimal Text from over the blockchain and convert it back to Alphanumeric Text
4. The recipient VTEP uses this data for further communications with all other VTEPs

Example:

[Figure 2] Customer #1555 LAN segment is connected to VTEP-1, VTEP-1 needs to participate in VXLAN with VNID 10123. VTEP-1 just learned the Media Access Control (MAC) address (00-14-22-01-23-45) from one of the locally attached servers belonging to Customer#1555 (Server-1 attached to Port 1/1).

The VTEP-1 IP address is 10.1.1.178, and this is the IP address that other VTEPs need to use to reach VTEP-1.  The message that will be published from that VTEP over the blockchain is typically a MAC-to-VTEP mapping message that also includes the Customer ID as well as the VNID.

1. VTEP Converts Alphanumeric Text to Hexadecimal Text
   1. From Alphanumeric Text: ‘customer 1555 vnid 10123 mac address 00-14-22-01-23-45 VTEP 10.1.1.178’
   2. To Hexadecimal Text: ‘637573746f6d6572203135353520766e6964203130313233206d616320616464726573732030302d31342d32322d30312d32332d343520565445502031302e312e312e313738’
2. VTEP Publishes Hexadecimal Text to Blockchain
3. VTEPs see the Blockchain Hexadecimal Text and reads them back all VTEPs
4. VTEPs Converts Hexadecimal Text to Alphanumeric Text
   1. From Hexadecimal Text: ‘637573746f6d6572203135353520766e6964203130313233206d616320616464726573732030302d31342d32322d30312d32332d343520565445502031302e312e312e313738’
   2. To Alphanumeric Text: ‘customer 1555 vnid 10123 mac address 00-14-22-01-23-45 VTEP 10.1.1.178’

[Figure 12] Hexadecimal Text Transmission

This message can be seen by all VTEPs participating in the blockchain but only those VTEPs that are interested in Customer ID 1555 and VXLAN VNID 10123 will use this message, translate it, and add its content to their local copy of the MAC-to-VTEP mappings.

[Figure 3] Because the different MAC-to-VTEP mappings are distributed over the blockchain to all participating nodes/VTEPs, as the final state.

* No data-plane learning is required for unknown unicast MAC addresses.
* No IP multicast underlay required. This is why BaaT can span beyond the boundary of a data center or cloud to the public Internet.
* Because of the distributed nature of blockchain, no significant delay is expected between the different nodes.
* For the broadcast and multicast traffic, the head-end replication is always the solution as in other control-plane-based VXLAN modes.

2.1    BACKGROUND: BaaT

* Seamless operation across  any IP transport network including the global public Internet.
* BaaT is an advanced L2VPN solution for both enterprises and telco/service providers,with which the organization can leverage the public Internet for their WAN traffic so that they don’t need to share traffic with their upstream providers as in the case of MPLS VPN service or even modern SD-WAN.
* Current physical or virtual devices support VXLAN and can accommodate the blockchain software.
* Unlike other tunneling techniques, BaaT is built to operate in a multipoint fashion. Its signaling is done separately via the blockchain and it has no scalability issues.
* No unknown unicast entry is to be found on any VTEPs; it’s either a unicast MAC address match,  advertised over the blockchain, or a default entry toward the VXLAN gateway.
* Multicast and broadcast traffic is handled via the head-end replication on the source VTEP to all other known VTEPs in the same VXLAN. The list of VTEPs is known - and always updated - over the blockchain.
* BaaT VPN
  + Security (Intranet/VPN)
    - Baat VPN leverages cryptography to encrypt data in the pipe and decrypt at the remote end
      * Thus, if anyone were to be able to intercept a payload of data, it would be encrypted.
    - Control Plane Security
      * All performed by the blockchain itself
      * Native security built into blockchain
      * VXLAN Security Field
        + A security layer nobody is using today
        + A field in the VXLAN header that we use
        + Encode VN ID in this security field
        + The node will discard the packet if this is zero
    - Data Plane Security
      * Encryption / Decryption
  + [Figure 26] Layer 2 VPN
    - Layer 2 (Data Link) – Carrier Grade Secure BaaT
      * BaaT leverages OpenCT blockchain to create an architecture that connects geographically dispersed layer-2 islands over any available infrastructure including the public Internet.
      * BaaT enhances the operation of VXLAN overlay networking technology by adding a control plane component to it and extending the VXLAN working domain beyond the boundary of a local data center or public cloud.
      * BaaT provides unique security strength:
        + Control and data planes are abstracted from the packet and each use a different encryption standard – SHA-256 for control plane and AES-256 for data plane.
        + Leverages cryptography (SHA-256) to create layer 2 tunnel endpoints (across the public Internet) – thus making encrypted tunnels that are invisible from a layer 3 perspective where hackers operate.

Impossible to see the control plane data from an IP perspective or from an IP packet perspective

* + - * + Private IP addresses and the associated VLANs for tunnel endpoints are encrypted via SHA-256. The only way to “participate” in a conversation is to be an authenticated node on the blockchain – via verified MAC address database.

Nodes in the network know about each other, and nodes not in the BaaT network cannot see the nodes in the network.

* + - * + Provides military grade end-to-end data encryption with negligible bandwidth tax on performance – 2% instead of standard of 20%.
      * BaaT scalability is superior to other tunneling techniques as it was built to operate in a multipoint fashion. It’s signaling is done separately via OpenCT blockchain and it has no scalability issues.
      * BaaT is an advanced L2 VPN solution for enterprises, governments, and telco/service providers, with which the organization can leverage the public Internet for their WAN traffic so that they don’t need to share traffic with their upstream providers as in the case of MPLS VPN service or even modern SD-WAN.
      * BaaT securely supports all kinds of network traffic including; Unicast, Multicast, and Broadcast.
      * BaaT treats the global Internet as a very big switch so that the environment leveraging BaaT remains like a switched environment although it may span the globe.
    - Enterprise VPN
      * [Figure 5] Hub Spoke
      * Multi Point (multiple locations connected to each other)
      * Facilitates secure transactions between facilities
    - Using blockchain as the security for the Units increases security of the components in the network
      * (Need full description of this concept, step by step)
    - Layer 3 Consumer BaaT (crypto VPN)
      * A blockchain based, cryptographically secured VPN
      * Global Road Warriors
        + Downloadable to your smartphone
        + Could be used like any VPN today
        + Military grade data encryption (AES-256)
        + Control plane layer abstraction (handled via OpenCT blockchain) ensures port level details are obfuscated.
        + Port-level obfuscation ensures inability for BaaT crypto VPN to be “blocked”.
        + Connect with discrete servers globally and appear as if they are in a different geographic area with no indication of port type activity (video streaming, file transfer, SMTP, etc.)
        + Usable on phone, tablet, PC, - using an application

1. DESCRIPTION: Blockchain-Defined WAN (BD-WAN)

BD-WAN is based on the well-known Software-Defined WAN (SD-WAN) architecture but with fine tuning and blockchain engagement.

The BD-WAN architecture resulting from the integration of blockchain with SD-WAN enables improved WAN services and secure Internet connectivity, making it competitive with more legacy WAN technologies such as dedicated links or MPLS. In some cases, it uses inexpensive Internet broadband connections to replace more expensive solutions.

BD-WAN Architecture components

* BD-WAN Controller: An SD-WAN controller that is northbound controlled via blockchain.
* BD-WAN Units: Customer Premises Equipment (CPE) installed to which the local WAN resources are directly connected (leased line, public internet, MPLS, wireless, satellite,etc.).
* Global Blockchain: In the BD-WAN, this is the OpenCT platform. The BD-WAN Controller and the BD-WAN units join the OpenCT blockchain.
* Load Balancing Gateway (LBG): a device that sits within the premises of partner networks.
* BD-WAN Secure Cloud: The interconnection with selected Public Clouds as well as Content Providers.
* BaaT allows for the secure communications between BD WAN Controller and BD WAN Units

The Evolution Of Networking:

[Figure 4] Comparing typical enterprise WAN solutions to the value

[Figure 5] SD-WAN services under a centralized control plane

[Figure 6] BD-WAN utilizing BD-WAN Controllers, BD-WAN Units, BD-WAN Cloud, CPE and LBG in .

The main features of the BD-WAN offerings are:

* Trusted per-usage billing (Bandwidth on demand) is verified and hard-coded over the blockchain.
  + Service being delivered to international carries
    - AT&T has something for small business under 500 Mbit - possibly just bandwidth throttling
  + This is multi gig solutions
    - Monitor application traffic
    - Based on what is needed against a threshold, a new smart contract is given, and a new request is made for a new lambda (optical network)
    - Uses predictive measures of the application to add optical lambdas
    - Works on the down side as well, turning off channels as necessary
    - Each blockchain based smart contract is the pricing index against the channels that are added or subtracted
    - All of this is automated, with no human interaction
    - Network intelligence to increase the bandwidth, and decreases in reverse
    - This is true bandwidth on demand
      * Consume what is needed, and pay for what is used
* The ability to establish and tear down logical as well as physical circuits, allowing the customers to pay only for what they consume -- no flat fee -- as well as minimizing international connectivity costs.This benefit is especially important when considering the high costs of trans-oceanic links, while allowing customers to scale up or burst connectivity during times of peak demand.
* Creative features by integrating blockchain with legacy technologies. For example, Inter-Domain MPLS traffic engineering can now be done via blockchain.
* Full visibility and control over all transport facilities either via Fiber to the Premises (FTTP) or via partnership with key telco operators and metro Ethernet providers worldwide.
* Removing expensive routing hardware by provisioning connectivity and services via the BD-WAN cloud and using commodity hardware at remote sites.
* Bringing public cloud services as well as content services seamlessly to the customers' doorstep as part of a standard WAN offering. BD-WAN customers don’t need to subscribe on their own with another public or content provider, as these services will be bundled in the BD-WAN service.

OpenCT Load Balancing Gateway (LBG) is a device that sits within the premises of our strategic partner networks. It’s main functions are:

* Support the registration process of new blockchain nodes for the partner’s end-clients.
* Translate from fiat, credit card, bank, multi-cryptocurrency exchange services, etc. into OCT Tokens. To mask the token utility process from an end-client perspective.
* Provide a buffer of tokens (between payment cycles) needed to unlock services subscribed by end-clients.
* Synchronize or route transactions between multiple private and public blockchains.
* Route services from other blockchains across OpenCT in support of OpenCT end clients.   
  Example: Golem network supports the distribution of inexpensive multithreaded compute services. These decentralized compute services can be routed through OpenCT’s LBG and delivered to end-clients.

BD-WAN architecture is based on the SD-WAN model and operates in a token-based approach. Customer units are installed on premises virtually use tokens to deal with the central controller in order to “unlock” their selected services thus controlling their usage and being able to select their services carefully.

3.2    BD-WAN Operation: Token Model Details

The BD-WAN CPE use crypto tokens to “virtually pay” for their communications with the BD-WAN Controller to unlock the service(s) they will use.

That is a crypto payment using the OCT token that’s the fuel of the OpenCT platform.

The crypto payments are all in the form of transactions happening on the blockchain (broadcasted to all nodes for further verification and for miners to pack them into proper blocks).

Inter-Domain MPLS Traffic Engineering.  A direct service that customers can leverage following their BD-WAN service subscription. Targeted to those customers who are running multiple MPLS clouds and still need to offer MPLS Traffic Engineering service across these MPLS clouds. MPLS Traffic Engineering operates seamlessly inside a single MPLS cloud but the Inter-Domain MPLS Traffic Engineering requires additional protocols to run, one of which is BGP-LS, that will be replaced by OCT blockchain in BD-WAN

As the different applications/traffic are asynchronous by nature -- no signaling to identify the exact amount to be sent -- the BD-WAN Units are required to pay at least the minimum amount for each service (minimum threshold).

3.3 BD-WAN Controller

* Controls every kind of component underneath it
  + The mind of all of the architecture
* Policies
* Open CT Routing Decisions
  + Background Info
    - Works within an existing vendor, and between vendors
    - Old School Fiber swapping, now it is at a specific block level
    - Traditional
      * Destination based, each routing decision is based on the destination, and each route forwards to the destination
      * Performance Based Routing (PBR)
        + QOS
        + Performance
        + Congestion (Performance)
    - SDWAN uses PBR and Traditional
    - OSPF / BGP Killer (what does this mean, what’s the difference?)
  + Open CT Routing Decision Factors
    - Traffic
      * Outage: Cables changing / can switch from broken cable (outage) to working cable in milliseconds
      * Performance: Can also switch to faster performing routes, not just broken routes
      * QOS - Quality of Service
    - Applications
      * VOIP
      * Data
      * Real Time
      * Class of packet: Applications
        + Critical / voice (video) vs. bulk payload vs. Video
    - Network Convergence
      * Outage
    - Internal Customer Policy
    - **Price**: Can also switch to lower cost routes, or higher quality higher priced routes
      * Time of day
* Inbound Request
* Ex: Communication between 2 branch offices
  + BD WAN unit will intercept the packet request
  + Branch 1 will send the header information to the BD WAN Controller along with signaling information
  + Based on the global map, controller will determine where to send the traffic based on efficiency
  + Controller will send info back to the BD WAN Unit
  + BD WAN Unit will take the necessary forwarding decision
* Fail over BD WAN Controllers as a Cluster (needs diagram update with multiple BD WAN Controllers as a Cluster)
  + Geographically separated
  + Act as failover

It is then the role of the BD-WAN Controller as well as the BD-WAN Units to set/reset special counters that will be used as reminders for ongoing payments required for smooth operation.

To ensure smooth and uninterrupted operation, the BD-WAN architecture follows the “fail-safe” approach, meaning that the operation continues as usual even if the Units don’t pay the Controller ontime.

[Figure 7] The BD-WAN Controller interoperates with the BD-WAN Unit from the Initial State

[Figure 8] To a Steady State where the counters are about to expire on the BD-WAN Controller and

[Figure 9] Another Steady State where the timers are about to expire on the BD-WAN units

[Figure 10] Interrupts are handled in .

[Figure 11] Conflicts on the BD-WAN Controller are handled in