CONSENSYS

EthOn - an Ethereum Ontology

Introducing semantic Ethereum

The author

Name:	Johannes Pfeffer
Ethereum account:	0xc656e934acee31f3d306142a020df5ae05f9880e
Works at:	ConsenSys LLC

What is EthOn?

5 facts about ethon

1. EthOn is an ontology
2. EthOn is an Ethereum reference
3. EthOn is a data model
4. EthOn a learning resource
5. EthOn is extensible

How EthOn was created

ing of this block
hich all fees

256-bit hash of the root
trie, after all transactions are
nalisations applied; formally H_r.

Root: The Keccak 256-bit hash of the
node of the trie structure populated with
ch transaction in the transactions list portion
of the block; formally H_t.

receiptsRoot: The Keccak 256-bit hash of the root node of the trie structure populated with the receipts of each transaction in the transactions list portion of the block; formally H_e.

logsBloom: The Bloom filter composed from indexable information (logger address and log topics) contained in each log entry from the receipt of each transaction in the transactions list; formally H_b.

difficulty: A scalar value corresponding to the difficulty level of this block. This can be calculated from the previous block's difficulty level and the timestamp; formally H_d.

number: A scalar value equal to the number of ancestor blocks. The genesis block has a number of zero; formally H_i.

gasLimit: A scalar value equal to the current limit of gas expenditure per block; formally H_l.

gasUsed: A scalar value equal to the total gas used in transactions in this block; formally H_g.

timestamp: A scalar value equal to the reasonable output of Unix's time() at this block's inception; formally H_s.

extraData: An arbitrary byte array containing data relevant to this block. This must be 32 bytes or fewer; formally H_x.

mixHash: A 256-bit hash which proves combined with the nonce that a sufficient amount of computation has been carried out on this block; formally H_m.

nonce: A 64-bit hash which proves combined with the mix-hash that a sufficient amount of computation has been carried out on this block; formally H_n.

The other two components in the block are si
list of ommer block headers (of the same form
and a series of the transactions. Formally

[2] ommer is the most prevalent (not
der_neutral_language#Family_Ter

, B_U)

om-

ceipt. In order to encode informa-
action concerning which it may be use-
ero-knowledge proof, or index and search,
a receipt of each transaction containing cer-
formation from concerning its execution. Each re-
ipt, denoted $B_R[i]$ for the ith transaction) is placed in
an index-keyed trie and the root recorded in the header as
H_e.

The transaction receipt is a tuple of four items comprising the post-transaction state, R_σ, the cumulative gas used in the block containing the transaction receipt as of immediately after the transaction has happened, R_u, the set of logs created through execution of the transaction, R_l and the Bloom filter composed from information in those logs, R_b:

$$R \equiv (R_\sigma, R_u, R_b, R_l) \qquad (19)$$

The function L_R trivially prepares a transaction receipt for being transformed into an RLP-serialised byte array:

$$L_R(R) \equiv (\mathtt{TRIE}(L_S(R_\sigma)), R_u, R_b, R_l) \qquad (20)$$

thus the post-transaction state, R_σ is encoded into a trie structure, the root of which forms the first item.

We assert R_u, the cumulative gas used is a positive integer and that the logs Bloom, R_b, is a hash of size 2048 bits (256 bytes):

$$R_u \in \mathbb{P} \quad \wedge \quad R_b \in \mathbb{B}_{256} \qquad (21)$$

The log entries, R_l, is a series of log entries, termed, for example, $(O_0, O_1, ...)$. A log entry, O, is a tuple of a logger's address, O_a, a series of 32-bytes log topics, O_t and some number of bytes of data, O_d:

$$O \equiv (O_a, (O_{t0}, O_{t1}, ...), O_d) \qquad (22)$$

$$O_a \in \mathbb{B}_{20} \quad \wedge \quad \forall_{t \in O_t} : t \in \mathbb{B}_{32} \quad \wedge \quad O_d \in \mathbb{B} \qquad (23)$$

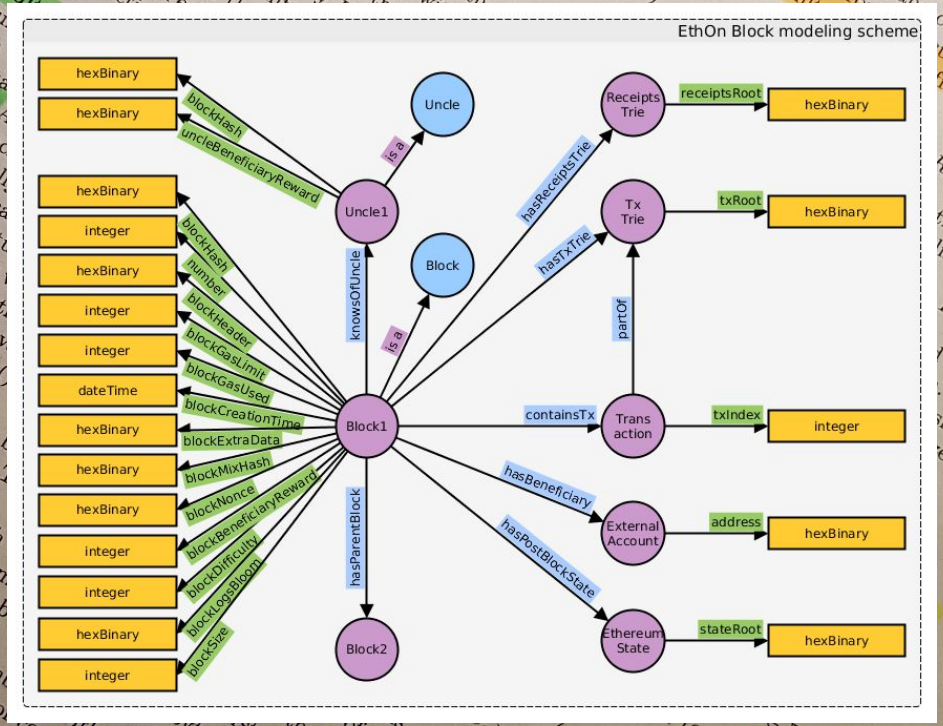
We define the Bloom filter function, M, to reduce a log entry into a single 256-byte hash:

$$M(O) \equiv \bigvee_{t \in \{O_a\} \cup O_t} \left(M_{3:2048}(t) \right) \qquad (24)$$

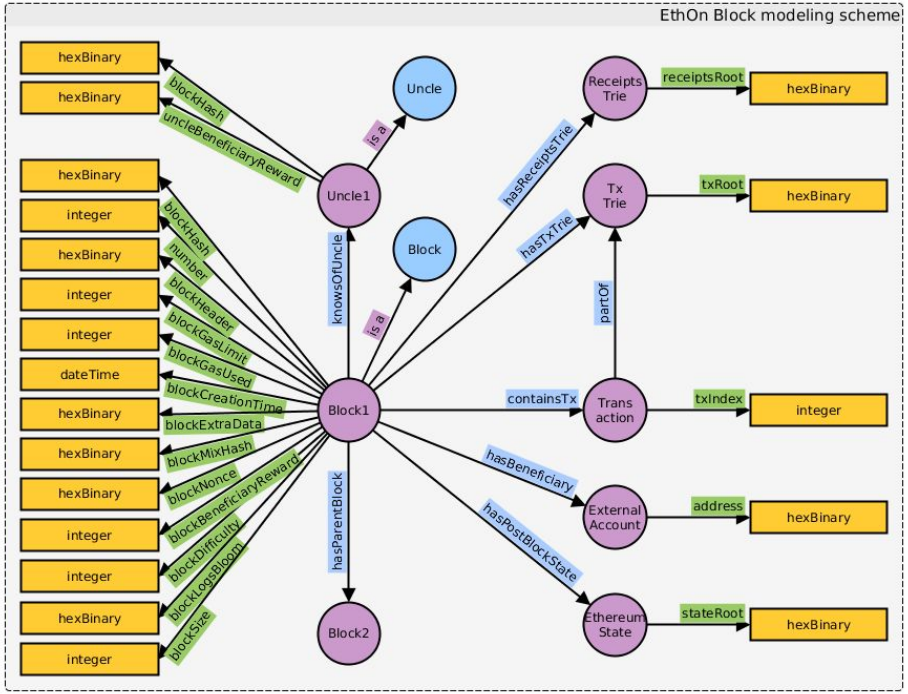
where $M_{3:2048}$ is a specialised Bl
three bits out of 2048, given an
does this through taking the
the first three pairs of by
byte series. Formally

(25) $M_{3:2048}($

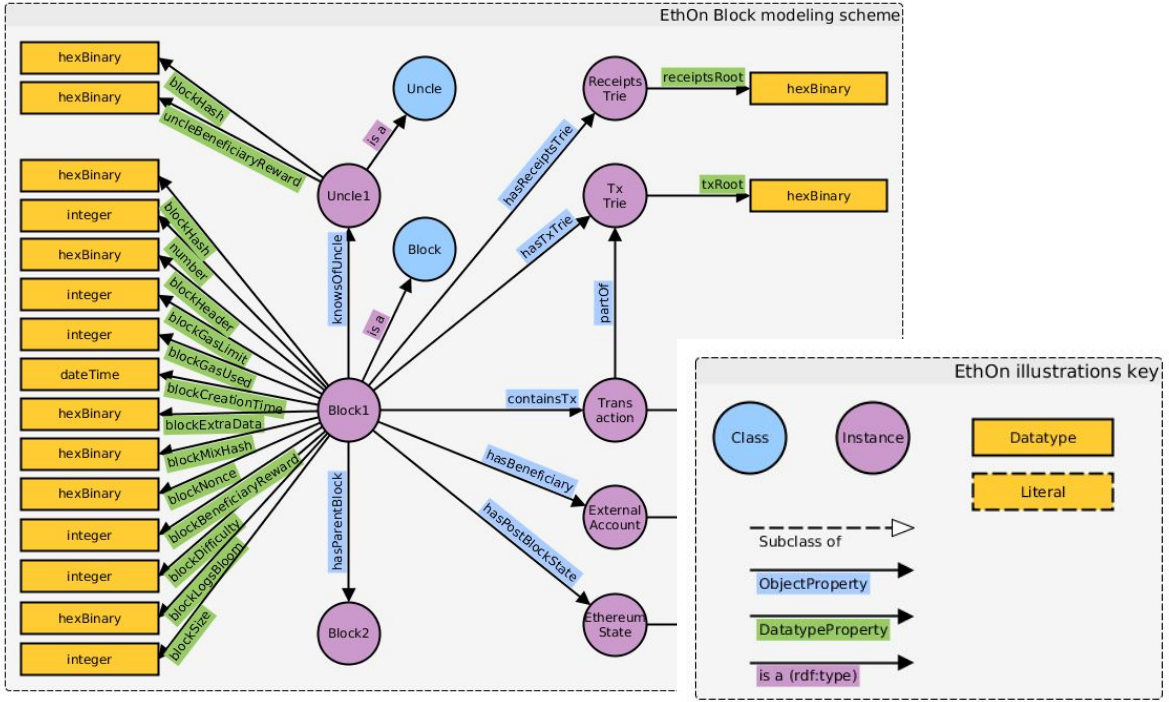
(26)


EthOn Block modeling scheme
hexBinary
hexBinary
blockHash
uncleBeneficiaryReward
Uncle
is_a
Uncle1
hexBinary
integer
hexBinary
integer
integer
dateTime
hexBinary
hexBinary
hexBinary
integer
integer
hexBinary
integer
blockHash
number
blockHeader
blockGasLimit
blockGasUsed
blockCreationTime
blockExtraData
blockMixHash
blockNonce
blockBeneficiaryReward
blockDifficulty
blockLogsBloom
blockSize
knowsOfUncle
Block
is_a
hasParentBlock
Block2
Block1
hasReceiptsTrie
hasTxTrie
partOf
containsTx
hasBeneficiary
hasPostBlockState
Receipts Trie
Tx Trie
Trans action
External Account
Ethereum State
receiptsRoot
hexBinary
txRoot
hexBinary
txIndex
integer
address
hexBinary
stateRoot
hexBinary

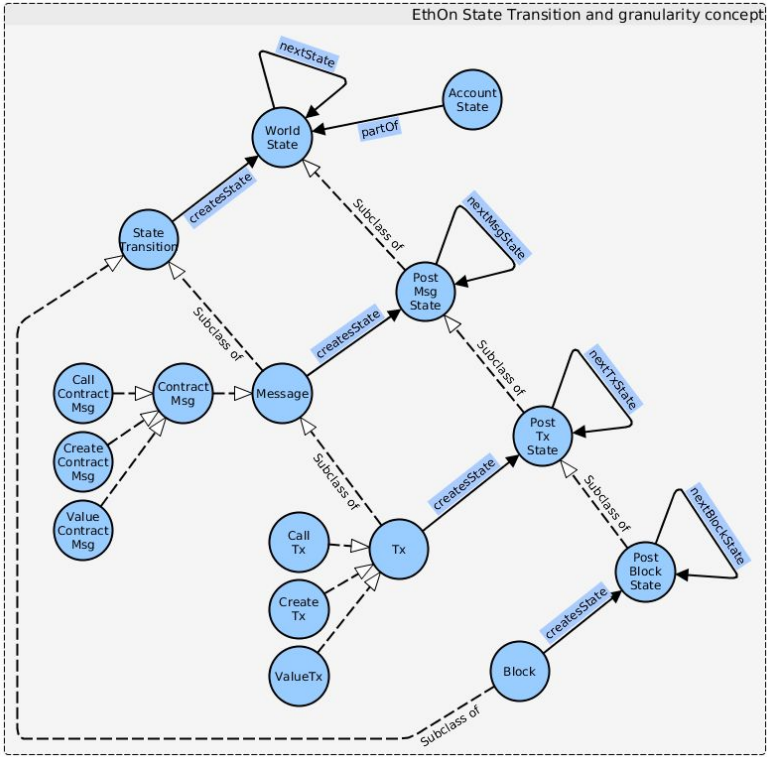
http://ethon.consensys.net/Block



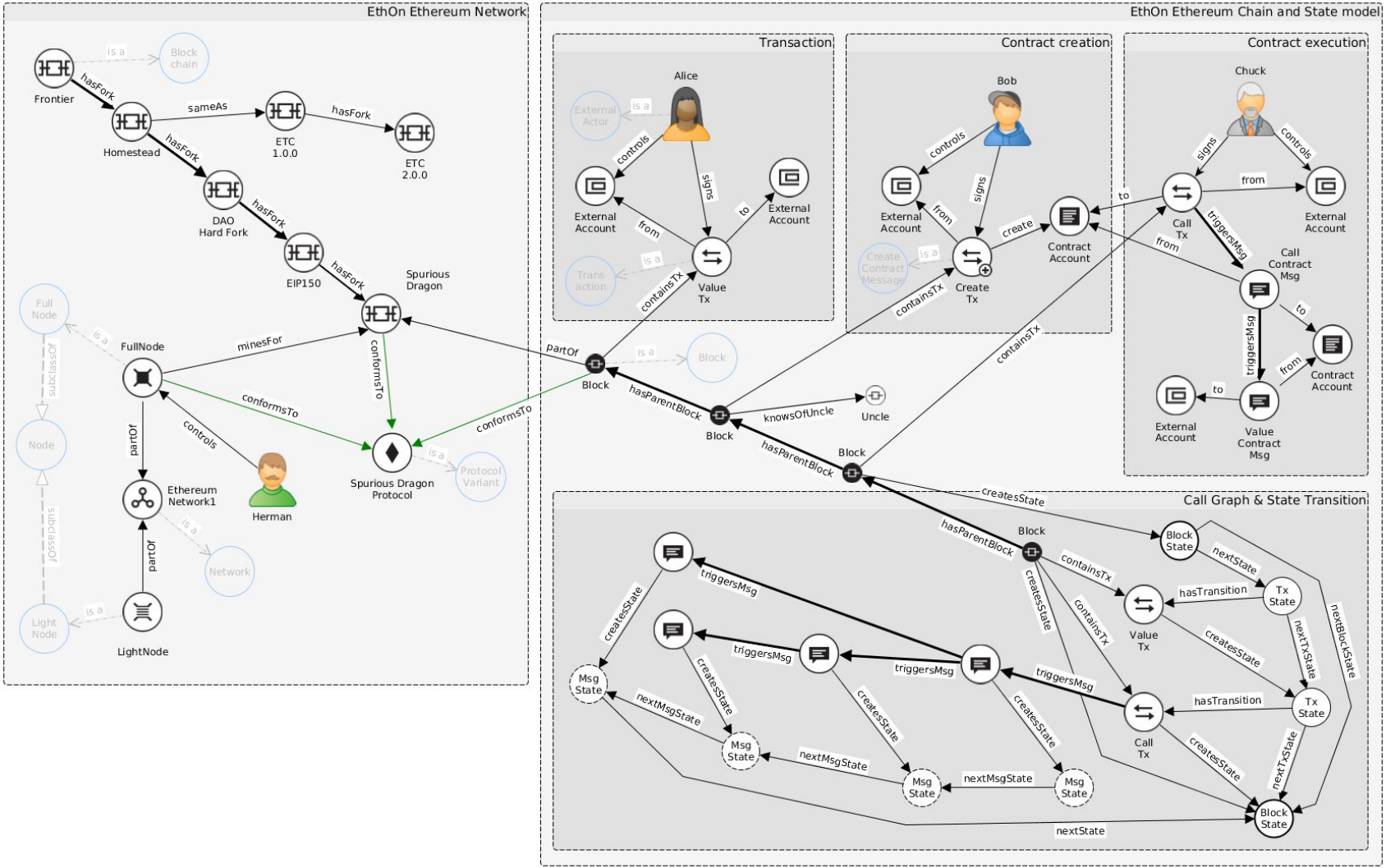
http://ethon.consensys.net/Block



http://ethon.consensys.net/StateTransition



What you can do with EthOn


EthOn Ethereum Network
Frontier
Homestead
ETC 1.0.0
ETC 2.0.0
DAO Hard Fork
EIP150
Spurious Dragon
Block chain
is a
hasFork
sameAs
Full Node
FullNode
minesFor
conformsTo
partOf
controls
Ethereum Network1
Herman
Spurious Dragon Protocol
Protocol Variant
Network
Node
Light Node
LightNode
subclassOf
EthOn Ethereum Chain and State model
Transaction
Alice
External Actor
External Account
Value Tx
controls
signs
from
to
containsTx
Contract creation
Bob
Create Tx
Contract Account
Create Contract Message
Trans action
Contract execution
Chuck
Call Tx
Call Contract Msg
Value Contract Msg
triggersMsg
Block
partOf
hasParentBlock
knowsOfUncle
Uncle
createsState
Call Graph & State Transition
Block State
Tx State
Msg State
Value Tx
Call Tx
nextState
hasTransition
nextTxState
nextBlockState
nextMsgState
triggersMsg

Formalize knowledge about Ethereum

```
ethereum:Block0
    a ethon:Block ;
    rdfs:label "Genesis Block" ;
    rdfs:comment "This is the block with block number 0. It is the Genesis Block of the Ethereum blockchain." ;
    ethon:number 0 ;
    ethon:hasBeneficary ethereum:Account0 ;
    ethon:blockBeneficiaryReward 5000000000000000000 ;
    ethon:blockGasLimit 5000 ;
    ethon:blockNonce "0000000000000042" ;
    [...]
    rdfs:seeAlso <https://etherscan.io/block/0> .
```

Exploit your knowledge

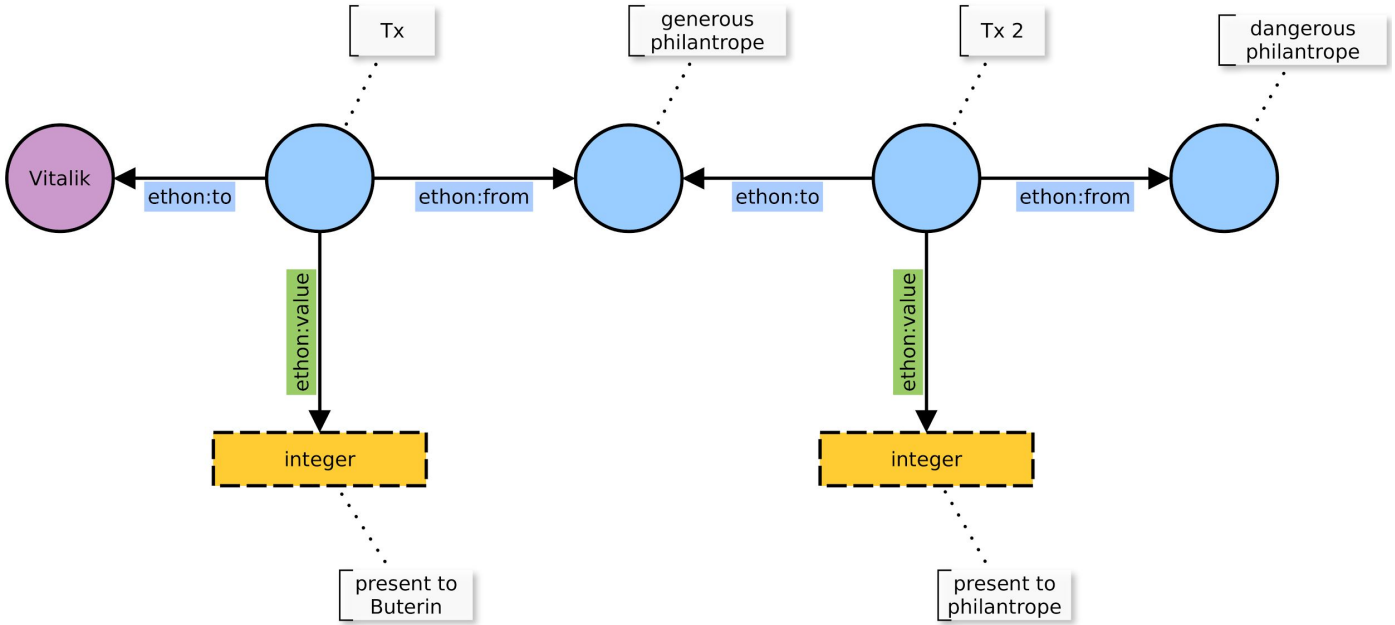
```
PREFIX ethon: <http://ethon.consensys.net/>
PREFIX etherscan: <https://etherscan.io/address/>

SELECT      ?generous_philantrope (SUM(?present_to_buterin) as ?direct_bribe)
            ?dangerous_philantrope (SUM(?present_to_philantrope) as ?indirect_bribe)
WHERE {
?tx   ethon:to etherscan:0xd8da6bf26964af9d7eed9e03e53415d37aa96045;  # Vitalik's Ethereum Account
      ethon:from ?generous_philantrope ;
      ethon:value ?present_to_buterin .

?tx2  ethon:to ?generous_philantrope ;
      ethon:from ?dangerous_philantrope ;
      ethon:value ?present_to_philantrope .
}
GROUP BY ?generous_philantrope ?dangerous_philantrope
```

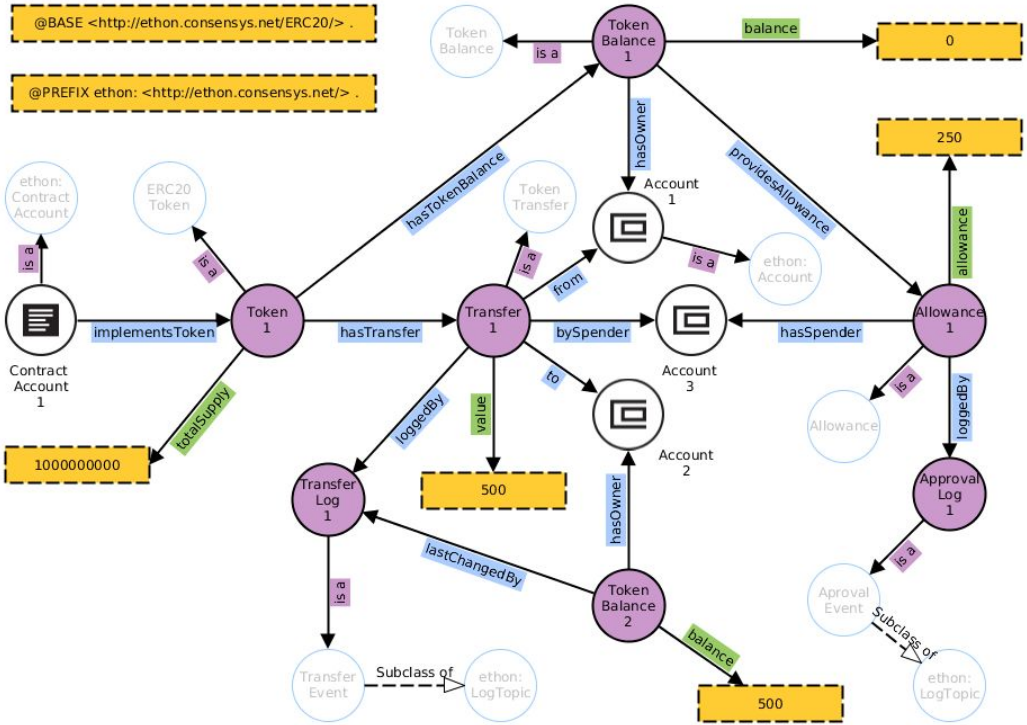
Exploit your knowledge

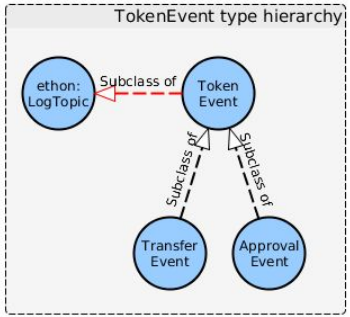
Visualized Query (QueryVOWL)

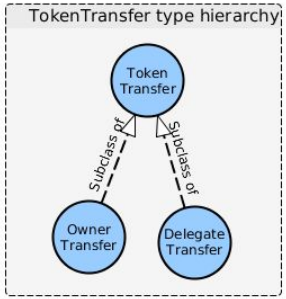


Even more of what you can do with EthOn

ERC20 extension







Afterwords

EthOn & Co.

EthOn main website:

http://ethon.consensys.net

EthOn - Introducing Semantic Ethereum (original article)

https://media.consensys.net/ethon-introducing-semantic-ethereum-15f1f0696986

Acknowledgements:

Alex Beregszaszi, Casey Detrio, Herman Junge, Joseph Chow, Maurycy Pietrzak, Marian Oancea, Niran Babalola, Shahan Khatchadourian, Stefano Bertolo

CONSENSYS