Estrazione di event log per process mining da ledger Algorand ed Ethereum Classic

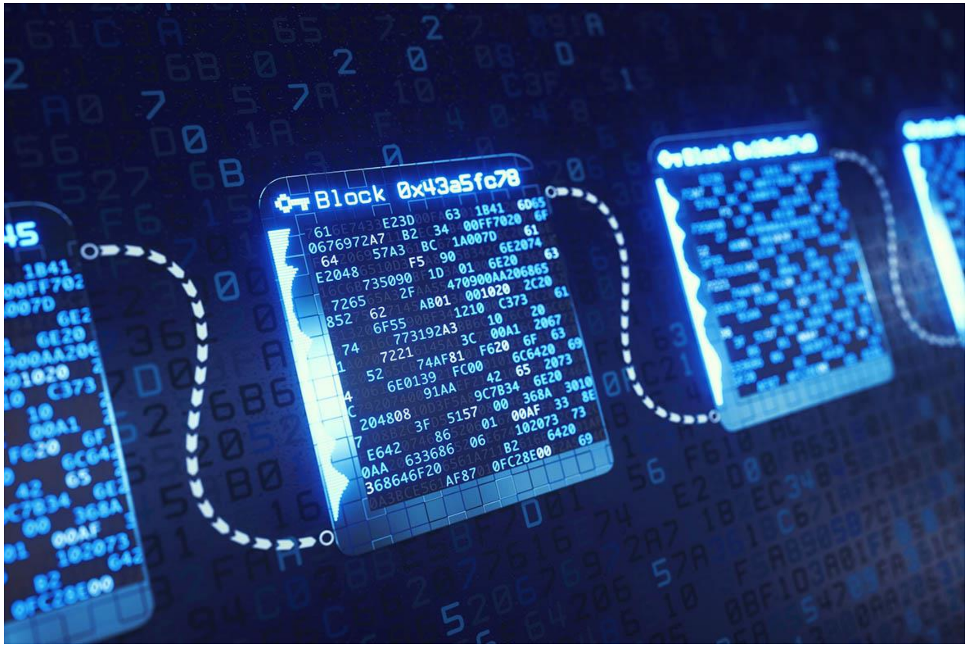
SAPIENZA
UNIVERSITÀ DI ROMA

Michele Kryston
1844733

Responsabile interno: Claudio Di Ciccio
Corso di Laurea in Informatica
Facoltà di Ingegneria dell’Informazione, Informatica e Statistica

Marzo 2022

Blockchain

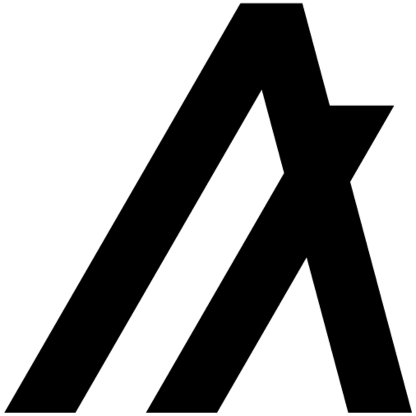


Fonte: https://authena.io/it/blockchain/

- ○ Trasparenza
- ○ Immutabilità
- ○ Sicurezza
- ○ Decentralizzazione
- ○ Privacy

Algorand

- Fondata da Silvio Micali nel 2017
- Proof of Stake
- Esecuzione di smart contracts (TEAL)
- Soluzione del trilemma?
  - Sicurezza
  - Scalabilità
  - Decentralizzazione



Fonte: https://cryptologos.cc/algorand

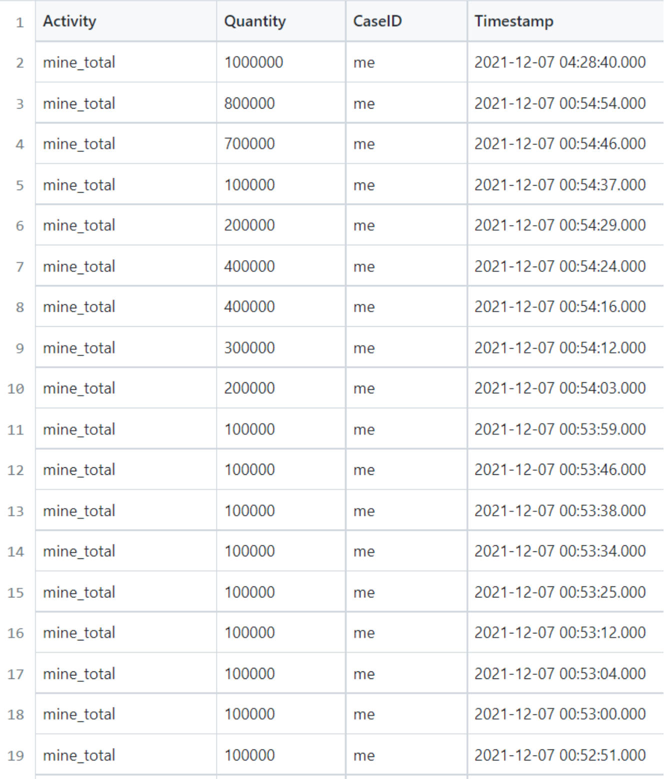
Ethereum Classic

Fonte: https://cryptologos.cc/ethereum-classic

- Fondata da Vitalik Buterin e Gavin Wood nel 2015
- Simile ad Ethereum (fork)
- Proof of Work
- Esecuzione di smart contracts (Solidity)

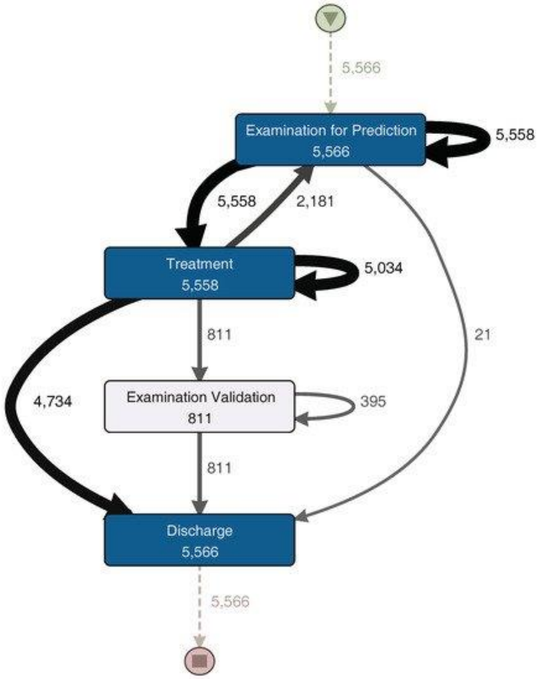
In Sintesi

Event log



Activity	Quantity	CaseID	Timestamp
mine_total	1000000	me	2021-12-07 04:28:40.000
mine_total	800000	me	2021-12-07 00:54:54.000
mine_total	700000	me	2021-12-07 00:54:46.000
mine_total	100000	me	2021-12-07 00:54:37.000
mine_total	200000	me	2021-12-07 00:54:29.000
mine_total	400000	me	2021-12-07 00:54:24.000
mine_total	400000	me	2021-12-07 00:54:16.000
mine_total	300000	me	2021-12-07 00:54:12.000
mine_total	200000	me	2021-12-07 00:54:03.000
mine_total	100000	me	2021-12-07 00:53:59.000
mine_total	100000	me	2021-12-07 00:53:46.000
mine_total	100000	me	2021-12-07 00:53:38.000
mine_total	100000	me	2021-12-07 00:53:34.000
mine_total	100000	me	2021-12-07 00:53:25.000
mine_total	100000	me	2021-12-07 00:53:12.000
mine_total	100000	me	2021-12-07 00:53:04.000
mine_total	100000	me	2021-12-07 00:53:00.000
mine_total	100000	me	2021-12-07 00:52:51.000

Modello di processo



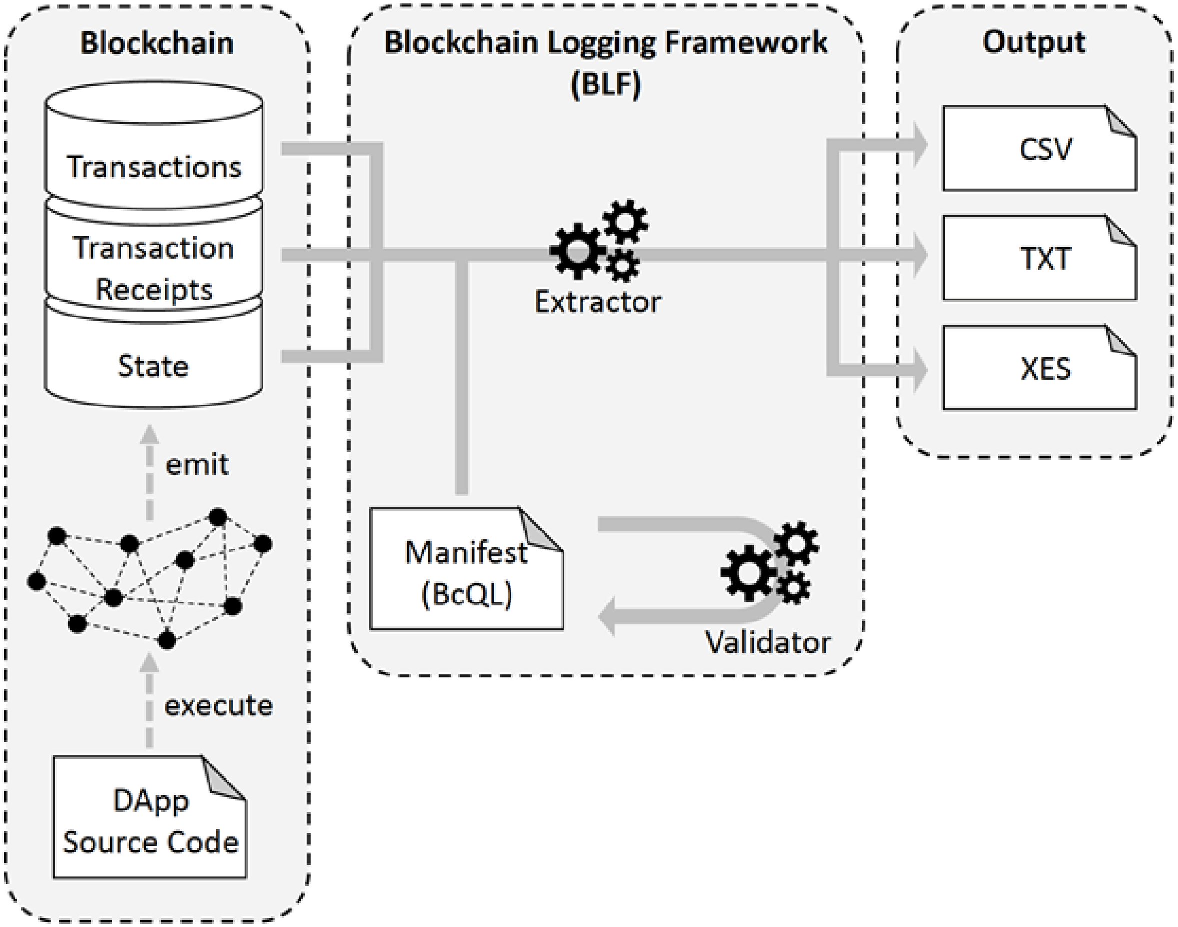
Fonte: https://www.mdpi.com/1660-4601/16/7/1274/htm

Blockchain Logging Framework [BLF]

- Applicazione per la creazione di event log a partire da transazioni su blockchain
- Supporta Ethereum e Hyperledger
- Fork di Ethereum Logging Framework
- Sviluppato da TU-Berlin Advanced Distributed System Prototyping
- Scritto in Java

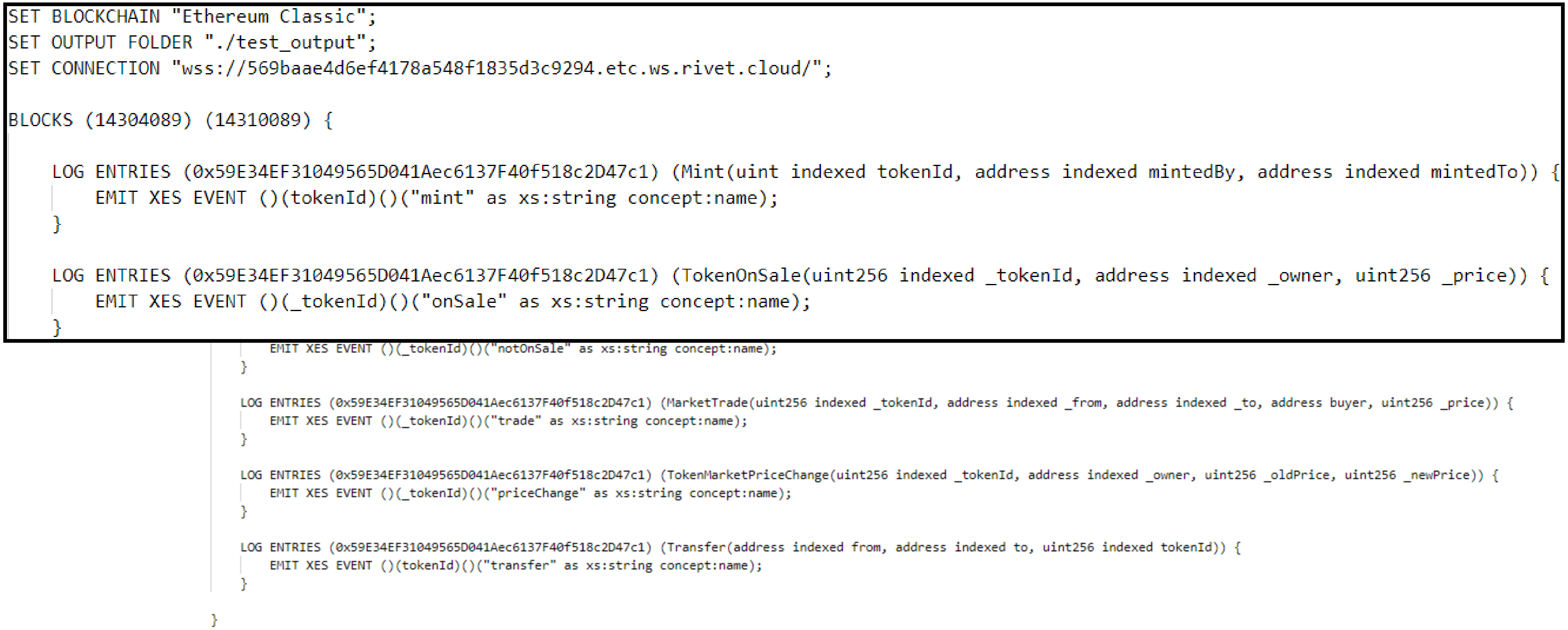
Fonti:
https://github.com/TU-ADSP
https://justech.altervista.org/java-per-principianti-introduzione-e-indice-dei-contenuti/

Sintesi del funzionamento di BLF



Fonte: https://github.com/TU-ADSP/Blockchain-Logging-Framework

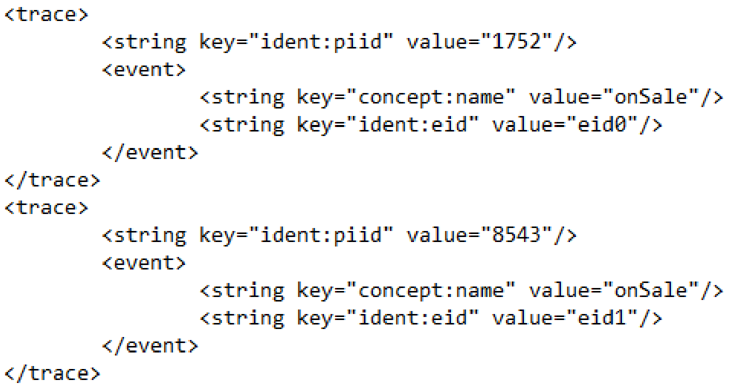
Input BLF [file manifest .bcql]



```
SET BLOCKCHAIN "Ethereum Classic";
SET OUTPUT FOLDER "./test_output";
SET CONNECTION "wss://569baae4d6ef4178a548f1835d3c9294.etc.ws.rivet.cloud/";

BLOCKS (14304089) (14310089) {

    LOG ENTRIES (0x59E34EF31049565D041Aec6137F40f518c2D47c1) (Mint(uint indexed tokenId, address indexed mintedBy, address indexed mintedTo)) {
        EMIT XES EVENT ()(tokenId)()("mint" as xs:string concept:name);
    }

    LOG ENTRIES (0x59E34EF31049565D041Aec6137F40f518c2D47c1) (TokenOnSale(uint256 indexed _tokenId, address indexed _owner, uint256 _price)) {
        EMIT XES EVENT ()(_tokenId)()("onSale" as xs:string concept:name);
    }
        EMIT XES EVENT ()(_tokenId)()("notOnSale" as xs:string concept:name);
    }

    LOG ENTRIES (0x59E34EF31049565D041Aec6137F40f518c2D47c1) (MarketTrade(uint256 indexed _tokenId, address indexed _from, address indexed _to, address buyer, uint256 _price)) {
        EMIT XES EVENT ()(_tokenId)()("trade" as xs:string concept:name);
    }

    LOG ENTRIES (0x59E34EF31049565D041Aec6137F40f518c2D47c1) (TokenMarketPriceChange(uint256 indexed _tokenId, address indexed _owner, uint256 _oldPrice, uint256 _newPrice)) {
        EMIT XES EVENT ()(_tokenId)()("priceChange" as xs:string concept:name);
    }

    LOG ENTRIES (0x59E34EF31049565D041Aec6137F40f518c2D47c1) (Transfer(address indexed from, address indexed to, uint256 indexed tokenId)) {
        EMIT XES EVENT ()(tokenId)()("transfer" as xs:string concept:name);
    }

}
```

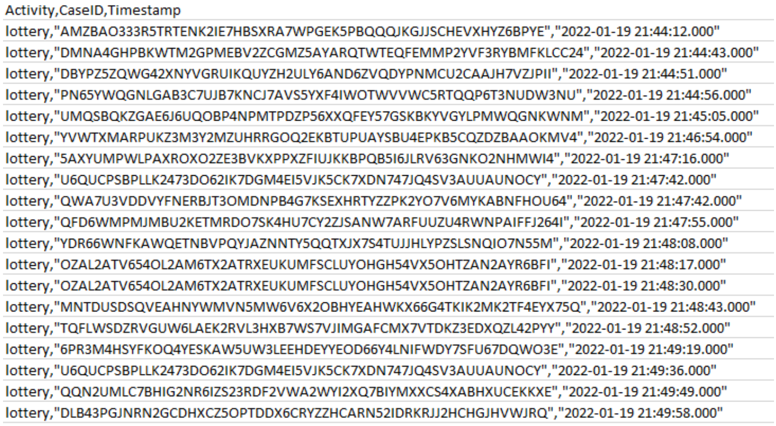
Output BLF

XES
Extensible Event Stream



```
<trace>
        <string key="ident:piid" value="1752"/>
        <event>
                <string key="concept:name" value="onSale"/>
                <string key="ident:eid" value="eid0"/>
        </event>
</trace>
<trace>
        <string key="ident:piid" value="8543"/>
        <event>
                <string key="concept:name" value="onSale"/>
                <string key="ident:eid" value="eid1"/>
        </event>
</trace>
```

CSV



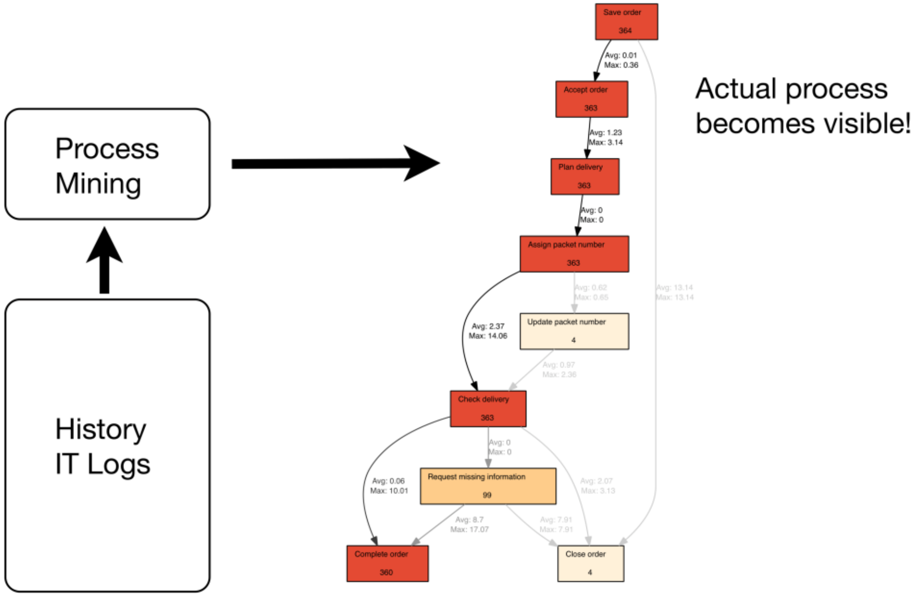
```
Activity,CaseID,Timestamp
lottery,"AMZBAO333R5TRTENK2IE7HBSXRA7WPGEK5PBQQQJKGJJSCHEVXHYZ6BPYE","2022-01-19 21:44:12.000"
lottery,"DMNA4GHPBKWTM2GPMEBV2ZCGMZ5AYARQTWTEQFEMMP2YVF3RYBMFKLCC24","2022-01-19 21:44:43.000"
lottery,"DBYPZ5ZQWG42XNYVGRUIKQUYZH2ULY6AND6ZVQDYPNMCU2CAAJH7VZJPII","2022-01-19 21:44:51.000"
lottery,"PN65YWQGNLGAB3C7UJB7KNCJ7AVS5YXF4IWOTWVVWC5RTQQP6T3NUDW3NU","2022-01-19 21:44:56.000"
lottery,"UMQSBQKZGAE6J6UQOBP4NPMTPDZP56XXQFEY57GSKBKYVGYLPMWQGNKWNM","2022-01-19 21:45:05.000"
lottery,"YVWTXMARPUKZ3M3Y2MZUHRRGOQ2EKBTUPUAYSBU4EPKB5CQZDZBAAOKMV4","2022-01-19 21:46:54.000"
lottery,"5AXYUMPWLPAXROXO2ZE3BVKXPPXZFIUJKKBPQB5I6JLRV63GNKO2NHMWI4","2022-01-19 21:47:16.000"
lottery,"U6QUCPSBPLLK2473DO62IK7DGM4EI5VJK5CK7XDN747JQ4SV3AUUAUNOCY","2022-01-19 21:47:42.000"
lottery,"QWA7U3VDDVYFNERBJT3OMDNPB4G7KSEXHRTYZZPK2YO7V6MYKABNFHOU64","2022-01-19 21:47:42.000"
lottery,"QFD6WMPMJMBU2KETMRDO7SK4HU7CY2ZJSANW7ARFUUZU4RWNPAIFFJ264I","2022-01-19 21:47:55.000"
lottery,"YDR66WNFKAWQETNBVPQYJAZNNTY5QQTXJX7S4TUJJHLYPZSLSNQIO7N55M","2022-01-19 21:48:08.000"
lottery,"OZAL2ATV654OL2AM6TX2ATRXEUKUMFSCLUYOHGH54VX5OHTZAN2AYR6BFI","2022-01-19 21:48:17.000"
lottery,"OZAL2ATV654OL2AM6TX2ATRXEUKUMFSCLUYOHGH54VX5OHTZAN2AYR6BFI","2022-01-19 21:48:30.000"
lottery,"MNTDUSDSQVEAHNYWMVN5MW6V6X2OBHYEAHWKX66G4TKIK2MK2TF4EYX75Q","2022-01-19 21:48:43.000"
lottery,"TQFLWSDZRVGUW6LAEK2RVL3HXB7WS7VJIMGAFCMX7VTDKZ3EDXQZL42PYY","2022-01-19 21:48:52.000"
lottery,"6PR3M4HSYFKOQ4YESKAW5UW3LEEHDEYYEOD66Y4LNIFWDY7SFU67DQWO3E","2022-01-19 21:49:19.000"
lottery,"U6QUCPSBPLLK2473DO62IK7DGM4EI5VJK5CK7XDN747JQ4SV3AUUAUNOCY","2022-01-19 21:49:36.000"
lottery,"QQN2UMLC7BHIG2NR6IZS23RDF2VWA2WYI2XQ7BIYMXXCS4XABHXUCEKKXE","2022-01-19 21:49:49.000"
lottery,"DLB43PGJNRN2GCDHXCZ5OPTDDX6CRYZZHCARN52IDRKRJJ2HCHGJHVWJRQ","2022-01-19 21:49:58.000"
```

Fonti:
https://www.tf-pm.org/newsletter/newsletter-stream-4-12-2020/10-years-of-xes
https://www.iconsdb.com/green-icons/csv-icon.html

Process Mining

Tre classi principali di tecniche di process mining:

- ○ Process Discovery
- ○ Conformance Checking
- ○ Performance Analysis



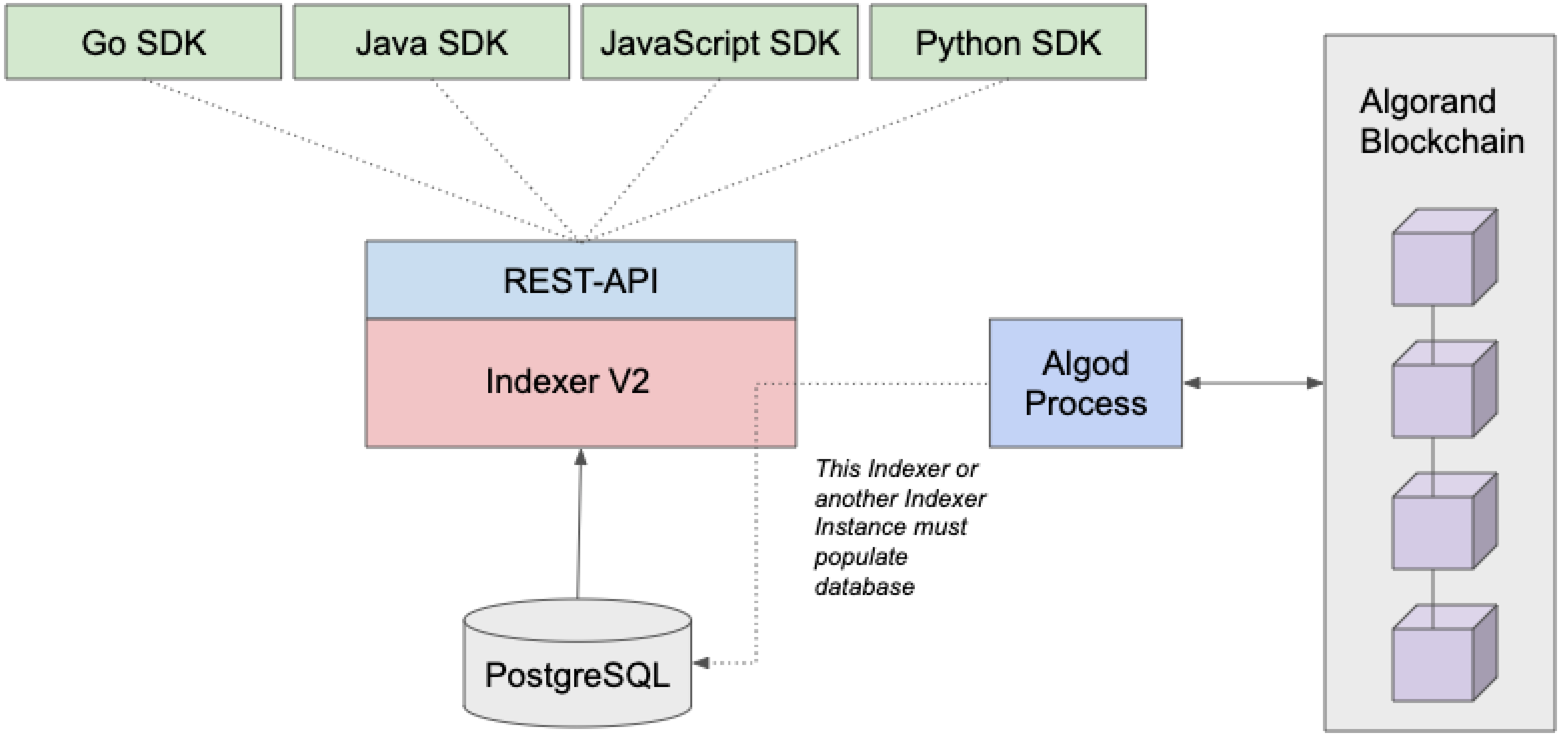
History IT Logs

Process Mining

Actual process becomes visible!

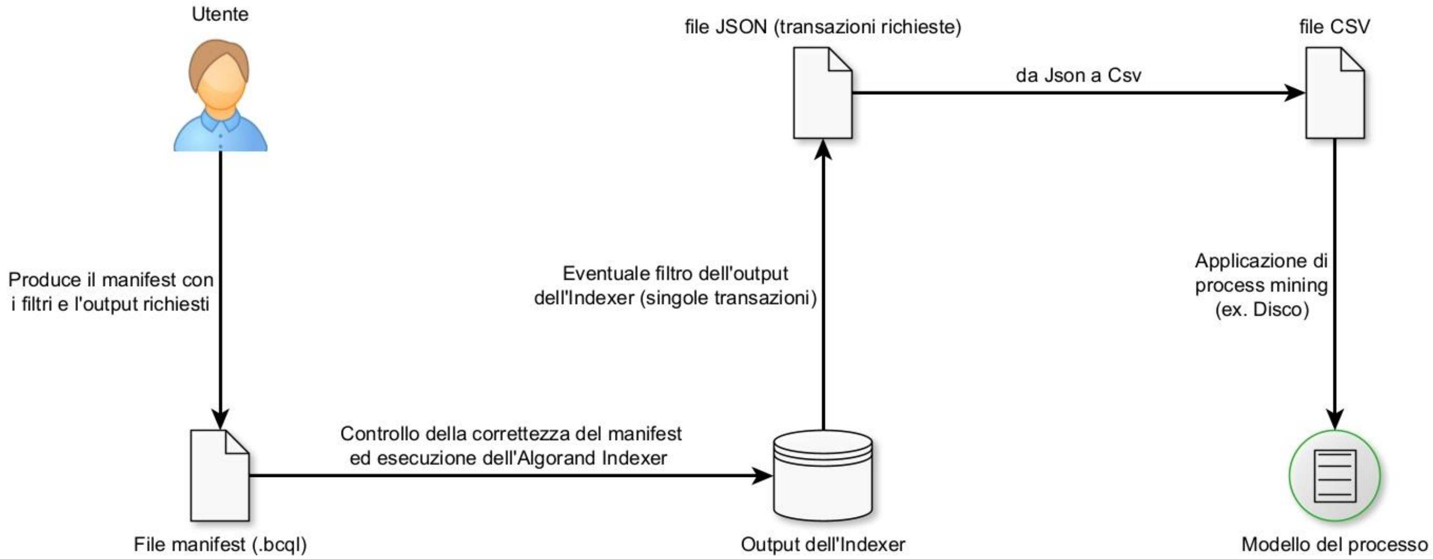
Fonte: https://fluxicon.com/blog/2011/05/transparency-the-greatest-benefit-of-process-mining/

Algorand Indexer



Fonte: https://developer.algorand.org/docs/get-details/indexer/

Implementazione di Algorand


Utente
file JSON (transazioni richieste)
file CSV
da Json a Csv
Produce il manifest con i filtri e l'output richiesti
Eventuale filtro dell'output dell'Indexer (singole transazioni)
Applicazione di process mining (ex. Disco)
Controllo della correttezza del manifest ed esecuzione dell'Algorand Indexer
File manifest (.bcql)
Output dell'Indexer
Modello del processo

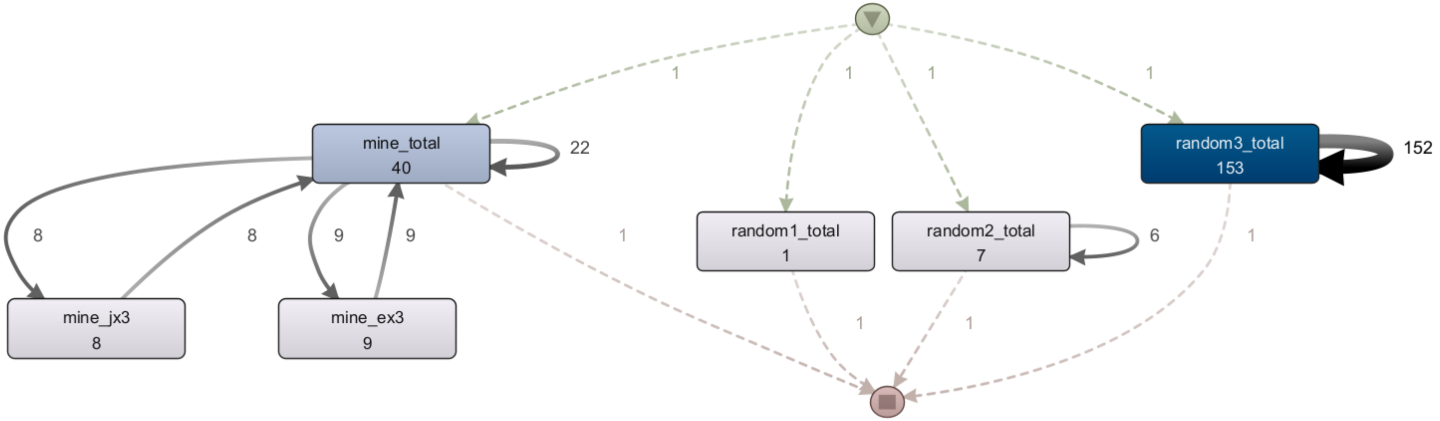
Implementazione di Ethereum Classic

- Implementazione semplice, BLF supporta già Ethereum (Solidity)
- Aggiunta di Ethereum Classic al validator (verifica il manifest)
- Utilizzo dello stesso extractor di Ethereum
- Collegamento ad un nodo di Ethereum Classic ed analisi dei blocchi

Fonti:
https://en.bitcoinwiki.org/wiki/Solidity
https://www.codeupset.com/why-web-application-programming-interface/

Analisi di un semplice scenario

Invio di ALGO sulla testnet di Algorand:

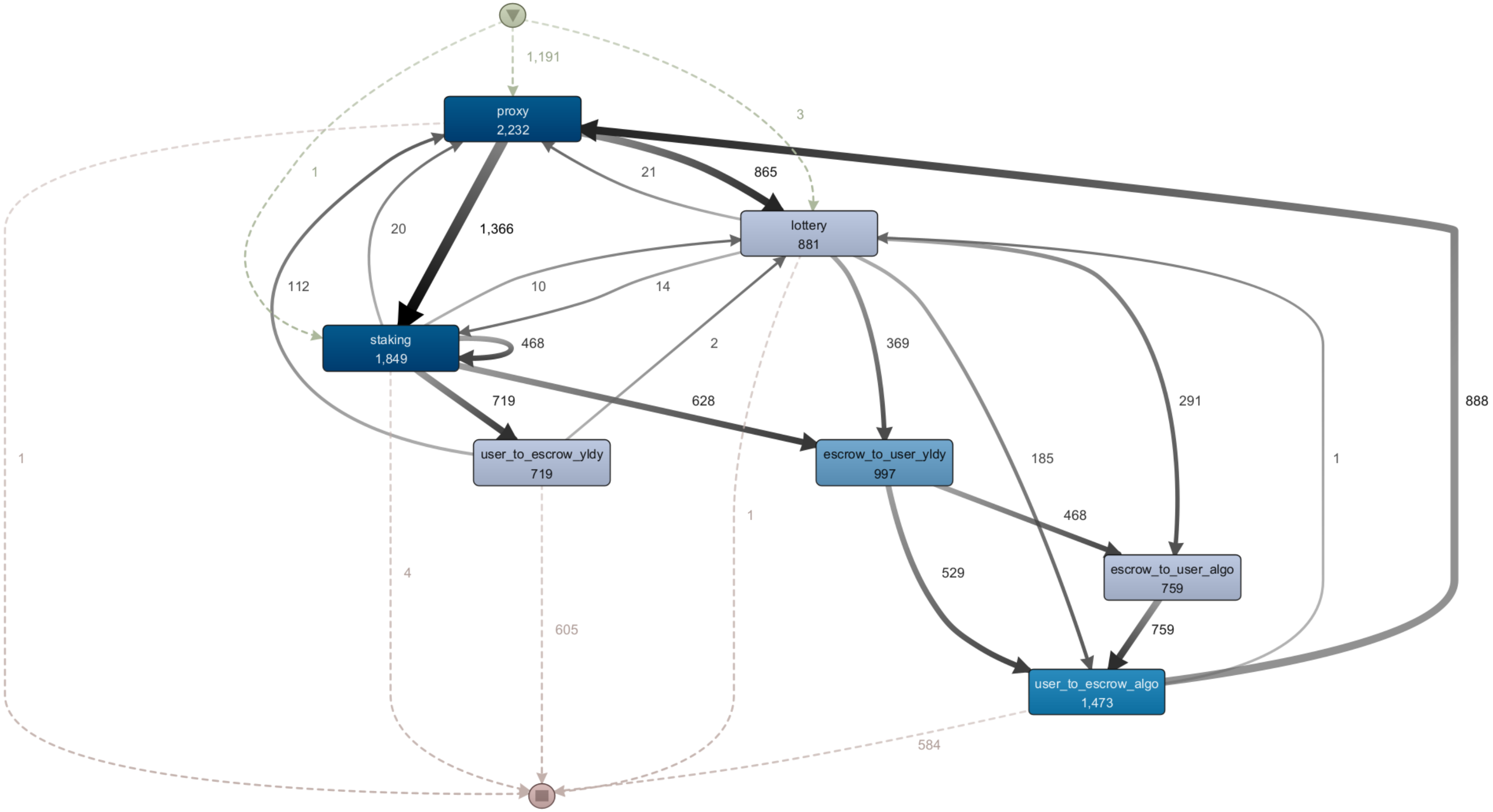


Dapp Yieldly.finance [Algorand]

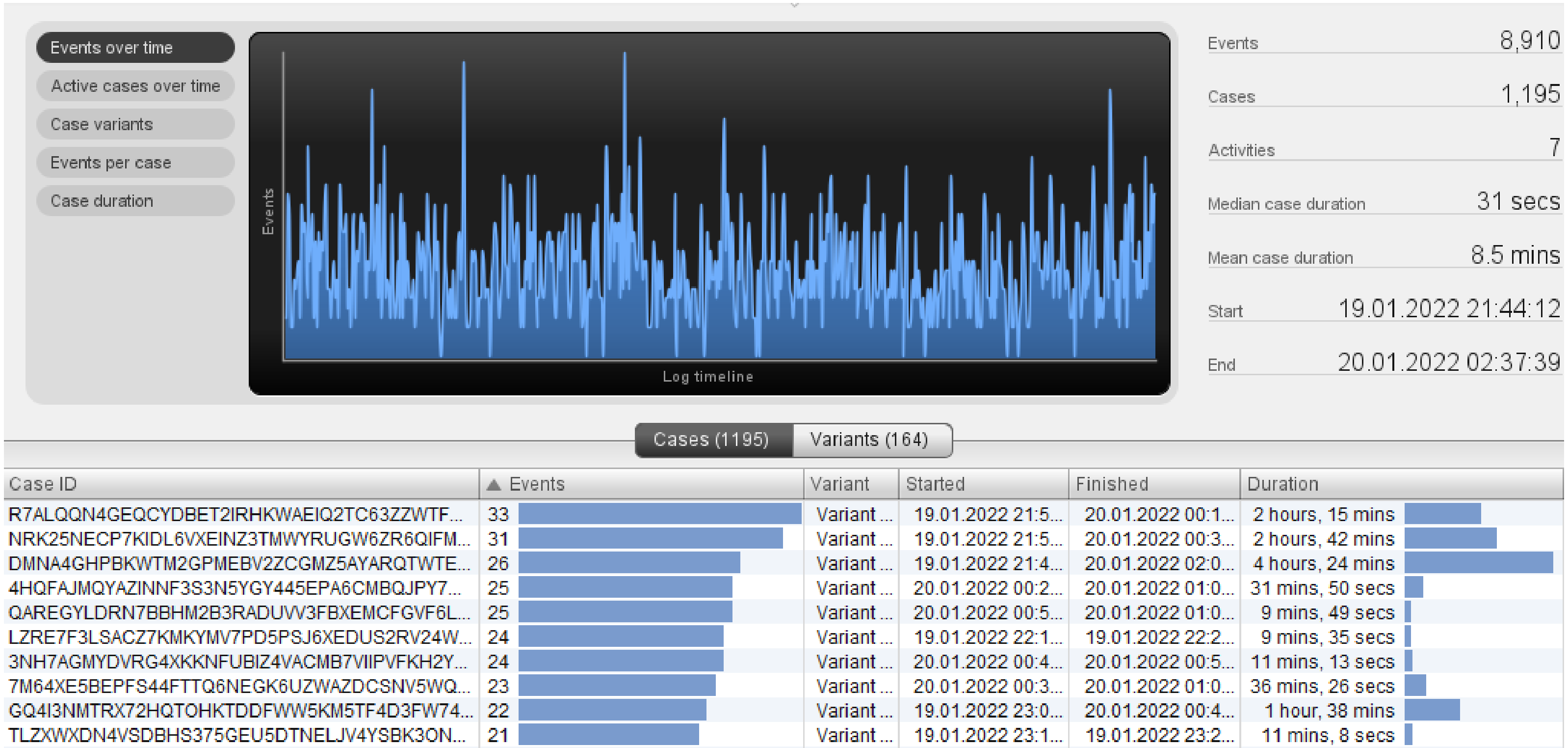
- Prima suite DeFi su Algorand
- Liquidity mining
- Lotteria no-lose
- Staking del token YLDY
- Swap cross-chain

Fonte: https://academy.moralis.io/blog/what-is-algorand-and-the-algo-token

Scenario Yieldly.finance [1/2]



Scenario Yieldly.finance [2/2]



Events	8,910
Cases	1,195
Activities	7
Median case duration	31 secs
Mean case duration	8.5 mins
Start	19.01.2022 21:44:12
End	20.01.2022 02:37:39

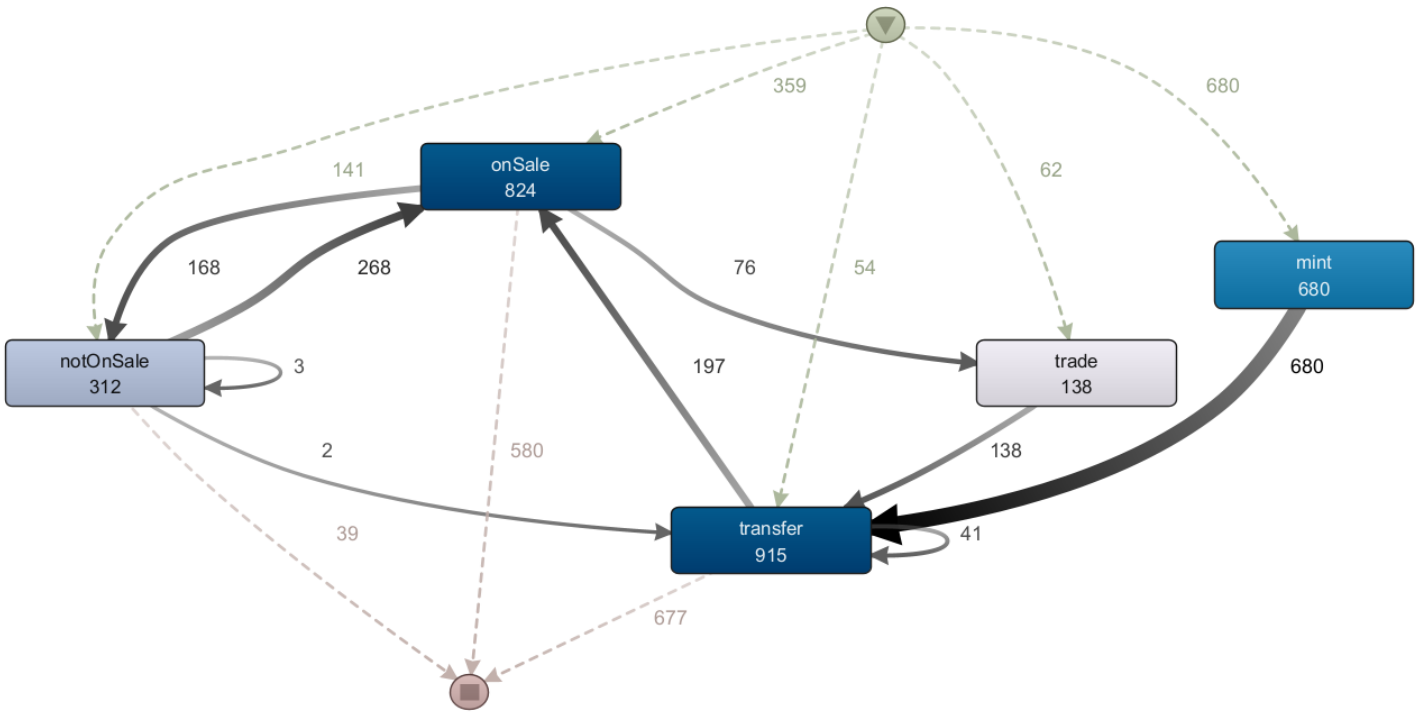
Case ID	▲ Events	Variant	Started	Finished	Duration
R7ALQQN4GEQCYDBET2IRHKWAEIQ2TC63ZZWTF...	33	Variant ...	19.01.2022 21:5...	20.01.2022 00:1...	2 hours, 15 mins
NRK25NECP7KIDL6VXEINZ3TMWYRUGW6ZR6QIFM...	31	Variant ...	19.01.2022 21:5...	20.01.2022 00:3...	2 hours, 42 mins
DMNA4GHPBKWTM2GPMEBV2ZCGMZ5AYARQTWTE...	26	Variant ...	19.01.2022 21:4...	20.01.2022 02:0...	4 hours, 24 mins
4HQFAJMQYAZINNF3S3N5YGY445EPA6CMBQJPY7...	25	Variant ...	20.01.2022 00:2...	20.01.2022 01:0...	31 mins, 50 secs
QAREGYLDRN7BBHM2B3RADUVV3FBXEMCFGVF6L...	25	Variant ...	20.01.2022 00:5...	20.01.2022 01:0...	9 mins, 49 secs
LZRE7F3LSACZ7KMKYMV7PD5PSJ6XEDUS2RV24W...	24	Variant ...	19.01.2022 22:1...	19.01.2022 22:2...	9 mins, 35 secs
3NH7AGMYDVRG4XKKNFUBIZ4VACMB7VIIPVFKH2Y...	24	Variant ...	20.01.2022 00:4...	20.01.2022 00:5...	11 mins, 13 secs
7M64XE5BEPFS44FTTQ6NEGK6UZWAZDCSNV5WQ...	23	Variant ...	20.01.2022 00:3...	20.01.2022 01:0...	36 mins, 26 secs
GQ4I3NMTRX72HQTOHKTDDFWW5KM5TF4D3FW74...	22	Variant ...	19.01.2022 23:0...	20.01.2022 00:4...	1 hour, 38 mins
TLZXWXDN4VSDBHS375GEU5DTNELJV4YSBK3ON...	21	Variant ...	19.01.2022 23:1...	19.01.2022 23:2...	11 mins, 8 secs

Dapp ETCBayc [Ethereum Classic]

- Progetto NFT su Ethereum Classic
- Dopo il grande successo di Bored Ape Yacht Club su Ethereum
- 10.000 NFT da collezionare e scambiare

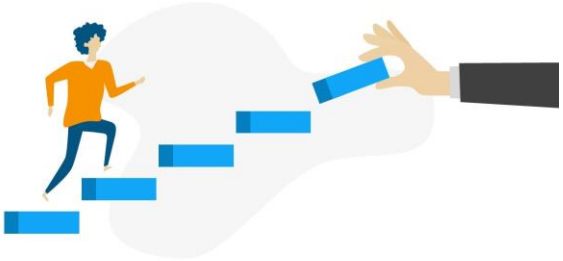
Fonti:
https://mobile.twitter.com/etcbayc/photo
https://etcbayc.com/detail/7495

Scenario ETCBayc



Sviluppi futuri

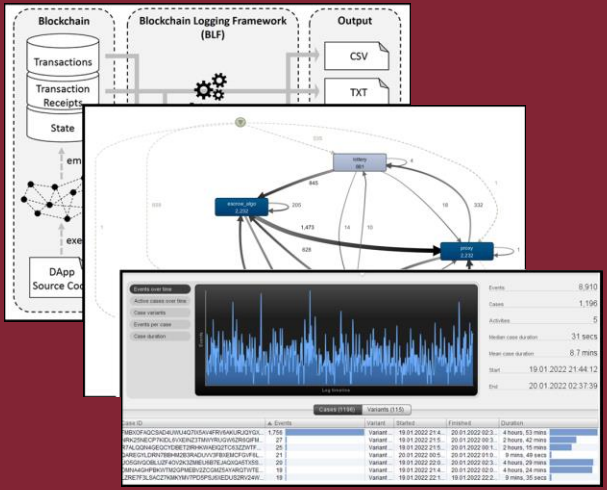
- ○ Implementare l’interfaccia grafica
- ○ Facilitare la generazione del file manifest
- ○ Migliorare il meccanismo di estrazione dati
- ○ Aggiungere ulteriori blockchain



Fonte: https://slidemodel.com/templates/whats-next-powerpoint-slides/

Estrazione di event log per process mining da ledger Algorand ed Ethereum Classic

Michele Kryston



Events 8,910
Cases 1,196
Activities 5
Median case duration 31 secs
Mean case duration 8.7 mins
Start 19.01.2022 21:44:12
End 20.01.2022 02:37:39

Case ID	Events	Variant	Started	Finished	Duration
TMBXOFAQCSAD4UWU4Q7IX5AV4FRV6AKURJQYQX...	1,756	Variant ...	19.01.2022 21:4...	20.01.2022 02:3...	4 hours, 53 mins
NRK25NECP7KIDL6VXEINZ3TMWYRUGW6ZR6QIFM...	27	Variant ...	19.01.2022 21:5...	20.01.2022 00:3...	2 hours, 42 mins
R7ALQON4GEQCYDBET2IRHKWAEIQ2TC63ZZWTF...	25	Variant ...	19.01.2022 21:5...	20.01.2022 00:1...	2 hours, 15 mins
QAREGYLDRN7BBHM2B3RADUVV3FBXEMCFGVF6L...	21	Variant ...	20.01.2022 00:5...	20.01.2022 01:0...	9 mins, 49 secs
UO5GIVQOBLUZF4OV2K3ZMEU6B7EJAQXQA5TX58...	20	Variant ...	19.01.2022 22:0...	20.01.2022 02:3...	4 hours, 29 mins
DMNA4GHPBKWTM2GPMEBV2ZCGMZ5AYARQTWTE...	19	Variant ...	19.01.2022 21:4...	20.01.2022 02:0...	4 hours, 24 mins
LZRE7F3LSACZ7KMKYMV7PD5PSJ6XEDUS2RV24W...	19	Variant ...	19.01.2022 22:1...	19.01.2022 22:2...	9 mins, 35 secs

SAPIENZA
UNIVERSITÀ DI ROMA

Codice open source:
https://github.com/IReallyLikeYourPants/Blockchain-Logging-Framework