DRAFT: PROJECT BRIEF – SETTLEMENT TOKEN FOR INTERBANK PAYMENTS

In a speech in late 2017, the Governor noted the possibility 'for the RBA to issue Australian dollars in the form of electronic files or tokens that could be used within specialised payment and settlement systems'. [1] He advised that the 'case for doing this has not yet been established, but we are open to the idea'. Following up on this, PY explored the possibility of a wholesale settlement token and, preliminarily, concluded that there was not a compelling case for the Bank to issue a new form of liability.[2] However, we noted that we planned to continue research in this area. The project described below would continue this research, exploring the policy case and the feasibility of using distributed ledger technology (DLT) for a new settlement token.

Policy questions

- Is there a case for issuing an RBA wholesale token that can be used for interbank wholesale settlement?
- What are the advantages and disadvantages of using DLT to issue a token for interbank settlement?

Objective

The project aims to build a small proof-of-concept (POC) of a digital token issued by the central bank, using DLT, that could be used to settle obligations between financial institutions. A number of central banks have conducted similar projects and reported on their results[3]. However, in some cases, a large share of the work has been done by external consultants rather than central bank staff. Moreover, the results from these experiments have been somewhat mixed. This POC will allow us to critically evaluate the results of those projects while providing practical (hands-on) experience with DLT. In addition, the POC should provide insights into how a central bank may issue a wholesale digital currency in a distributed ledger. To maximise the practical experience benefits of the POC, PY staff would need to be involved in every step of the process.

Plain-vanilla POC

The POC will simulate a small financial system with a few commercial banks and a central bank. The commercial banks make transactions between themselves using the token created by the central bank. The basic POC will involve a permissioned Ethereum network with a minimum of 5 simulated banks (nodes) each validating and making transactions. The basic simulation would have four stages:

1. **Creation**: The central bank creates the tokens at the start of the day.
2. **Distribution**: The central bank distributes the tokens across the banks.
3. **Use**: The banks send tokens to each other in payment for obligations agreed outside the system.
4. **Redemption**: At the end of the day the banks send the tokens back to the central bank to be redeemed.

To keep the project simple, the central bank would use an 'omnibus' account for the tokens (instead of individual accounts for each participant). This means the central bank knows how many tokens are in existence, and who 'purchased' them at the start, but does not know who owns them (during the day) until

[1] Lowe P (2017), 'An eAUD?', Address to the 2017 Australian Payment Summit, Sydney, 13 December.
[2] Thompson C, L Jiamin, E Tellez (2018), 'An eAUD for Business-to-Business Use?', PY Note, 15 March.
[3] For example, the Bank of Canada (Project Jasper), the European Central Bank and Bank of Japan (Project Stella), the Monetary Authority of Singapore (Project Ubin) and the Reserve Bank of South Africa (Project Khokha).

they are redeemed. This setup also avoids the issue of having to reconcile individual accounts at the central bank after each trade between participants.

Expected output

- Working prototype. While it could be useful for the prototype to include a basic user interface, it is not a core objective of the project.
- Paper covering the prototype, key results and lessons learned.

Timeframe and resources

The project will require three staff over three months: one nearly full time staff with IT technical skills, to do the coding in Ethereum, and two part time staff from PY, to provide economic intuition in the design and lead the drafting of the results paper.

DLT Technology

The POC will be initially based on Ethereum DLT technology, as a private network. As the most popular technology for smart contracts, Ethereum is a useful baseline platform for developing a greater understanding of how DLT technologies function. It also has a large user base offering greater support and 'how-to' guides for its use. An alternative choice would be to use JP Morgan's Quorum technology. This is a modified version of Ethereum designed for creating permissioned DLT networks, forgoing the mining consensus mechanism.

Infrastructure

The underlying infrastructure to support the DLT environment fits well with the use of Cloud Technology. Amazon Web Services (AWS) is a common choice for DLT technology test environments, and would be well placed in providing an elastic (can grow and shrink based on demand), agile (can be reconfigured/provisioned quickly and easily based on technological need) and programmable infrastructure. This means that the solution can be stopped, started, redeployed and rescaled based on need in a repeatable fashion. Alternatively, the POC could be stood up on a local environment or a more permanent internal VM, however this would introduce problems in scaling the solution for testing different scenarios (such as node removal or scaling simulations).

Setup/Interfacing

There are a few ways to interface and interact with the PoC

- **Wallet GUI (Graphical User Interface)** - A wallet program can be setup to view token balances and contracts in the private network
- **Console** - Logging into each 'node' on the network would allow to enter commands to directly interface with the Ethereum Network. This can be used as a simple way to make monetary transactions.
- **'Control' website GUI** - As mentioned earlier, a basic user interface could prove useful for the functionality and demonstrability of the PoC, and a friendlier way of making transactions and contract operations. A GUI can be setup on a node on the network, allowing for a website to trigger transactions or testing functions. This would essentially be a javascript-based website running on each node of the network that has a subset of commands relevant to its role. A GUI could also be useful for exploring the history of transactions and balances across the network.

Appendix: Possible extensions

- Replicate the POC in distributed ledger platforms that have been specifically designed for financial applications, such as Corda or Quorum. This would allow to compare the performance of the different platforms and better understand their strengths and weaknesses across a number of dimensions such as privacy and scalability.
- Invite external banks to participate in the project. This would include the banks pledging (simulated) central bank reserves on a one-to-one basis in exchange for the tokens (not necessarily in equal amounts across banks). The tokens would be exchanged between banks in payment of (simulated) obligations (agreed at the start of the experiment). During the day the banks would also have the option of 'cashing out' by sending the tokens back to the central bank.
- Extensions for a second phase of the project could include introducing more realistic transaction volumes, liquidity saving mechanisms and/or other assets to simulate delivery versus payment (DvP).
- Include the possibility that the central bank pays interest on the digital token (including positive and negative interest). The ability to pay interest on the token has important implications for monetary policy and the POC should help our understanding of its practical complexities. There are many questions, for example: How is the interest calculated? How would the central bank reduce token values to account for negative interest?

Settlement Token

18 July 2019
Head Office

Blockchain basics

- **Blockchain**: a distributed ledger of all transactions that have occurred on the network
  - Transactions are grouped into blocks
- **Nodes**: user devices connected to the blockchain
- **Mining**: the process by which blocks are added to the blockchain
- **Block height**: the number of blocks in the blockchain
  - No centralised concept of time
- **Fork**: a temporary split in the blockchain
  - Occurs when multiple blocks are mined simultaneously
  - Theoretically, no **finality** for blockchain transactions

Ethereum basics

- All activity is visible to others on the blockchain
- Participants may have multiple identities/addresses, which are represented as alphanumeric strings on the blockchain
- Mining is based on a **proof of work** consensus mechanism
- Blocks are added every 12 seconds on average

Demonstration timeline

10:00PM – 7:00AM

↓

Trading closed

No trading or approvals.

Commercial banks can request accounts and tokens.

7:00AM

→

Approvals open

Central Bank can now approve commercial banks' account and token requests.

Commercial banks can continue to make requests.

7:30AM

↑

Trading opens

Commercial banks can continue to make requests. They can now redeem tokens as well.

Commercial banks can transfer tokens.

7:30AM – 10:00PM

↑

Trading open

Commercial banks request addresses, request tokens, redeem tokens and transfer tokens as required.

10:00PM

↓

Trading closes

Commercial banks can no longer transfer or redeem tokens.

Central Bank will not approve requests until Approvals open the next day.

10:00 – 11:00PM

↓

Sweep

Central Bank destroys on-chain tokens.

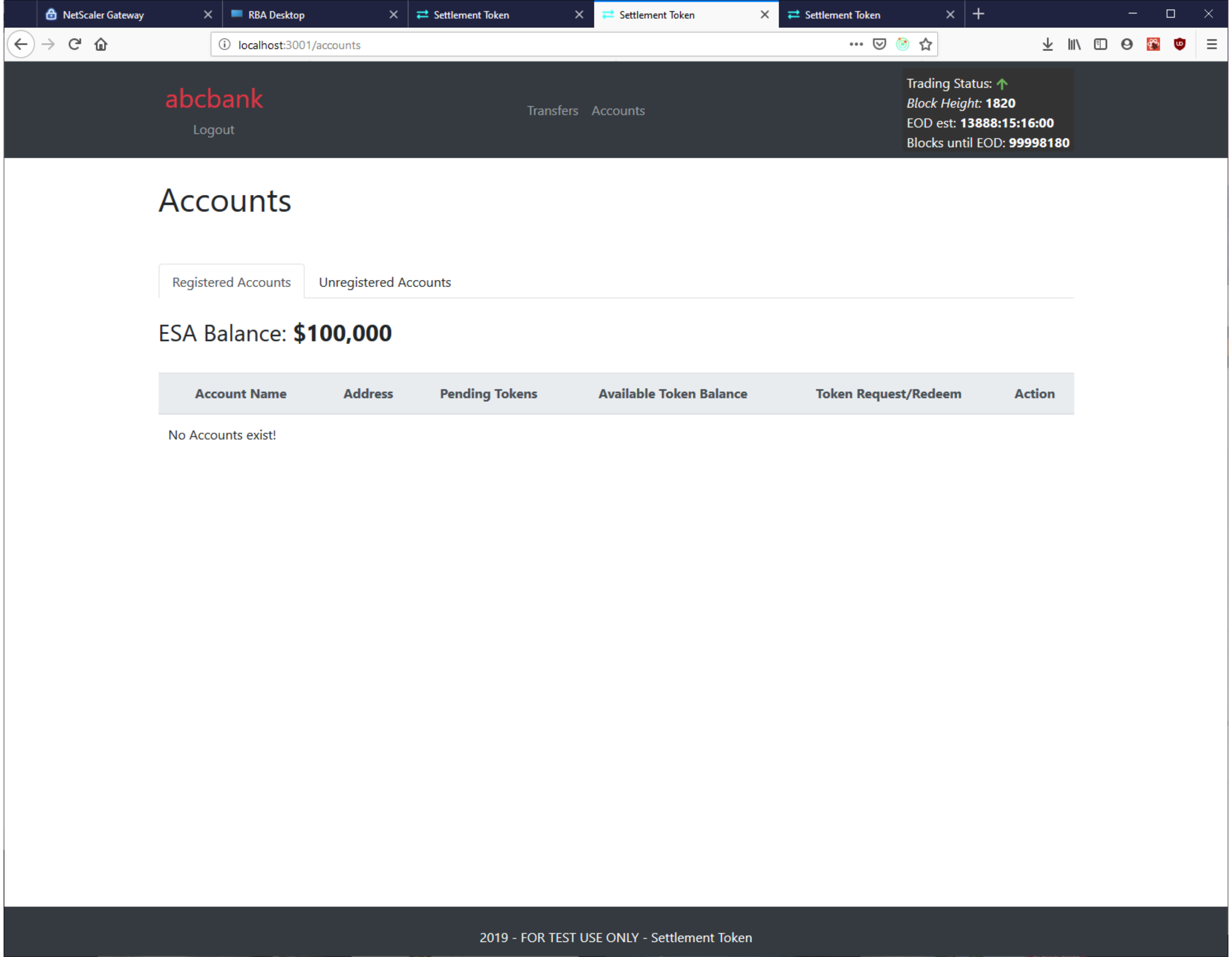
The Central Bank then initiates a balance by returning funds to respective ESAs.

Day 0

Adding accounts

Day 0

ABC Bank registers an account on the blockchain



Trading Status: ↑
Block Height: **1820**
EOD est: **13888:15:16:00**
Blocks until EOD: **99998180**

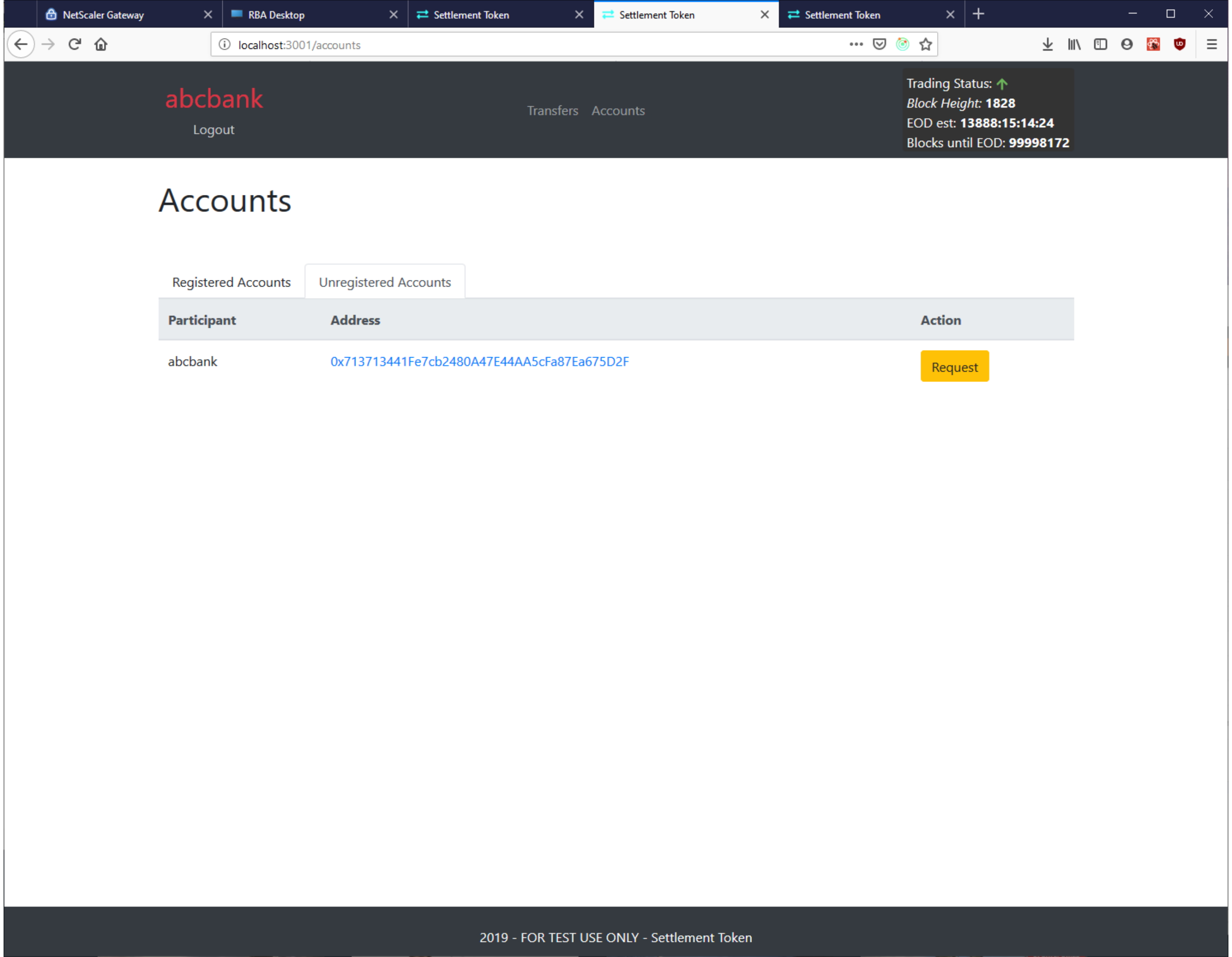
Accounts

Registered Accounts | Unregistered Accounts

ESA Balance: **$100,000**

Account Name	Address	Pending Tokens	Available Token Balance	Token Request/Redeem	Action
No Accounts exist!					

2019 - FOR TEST USE ONLY - Settlement Token

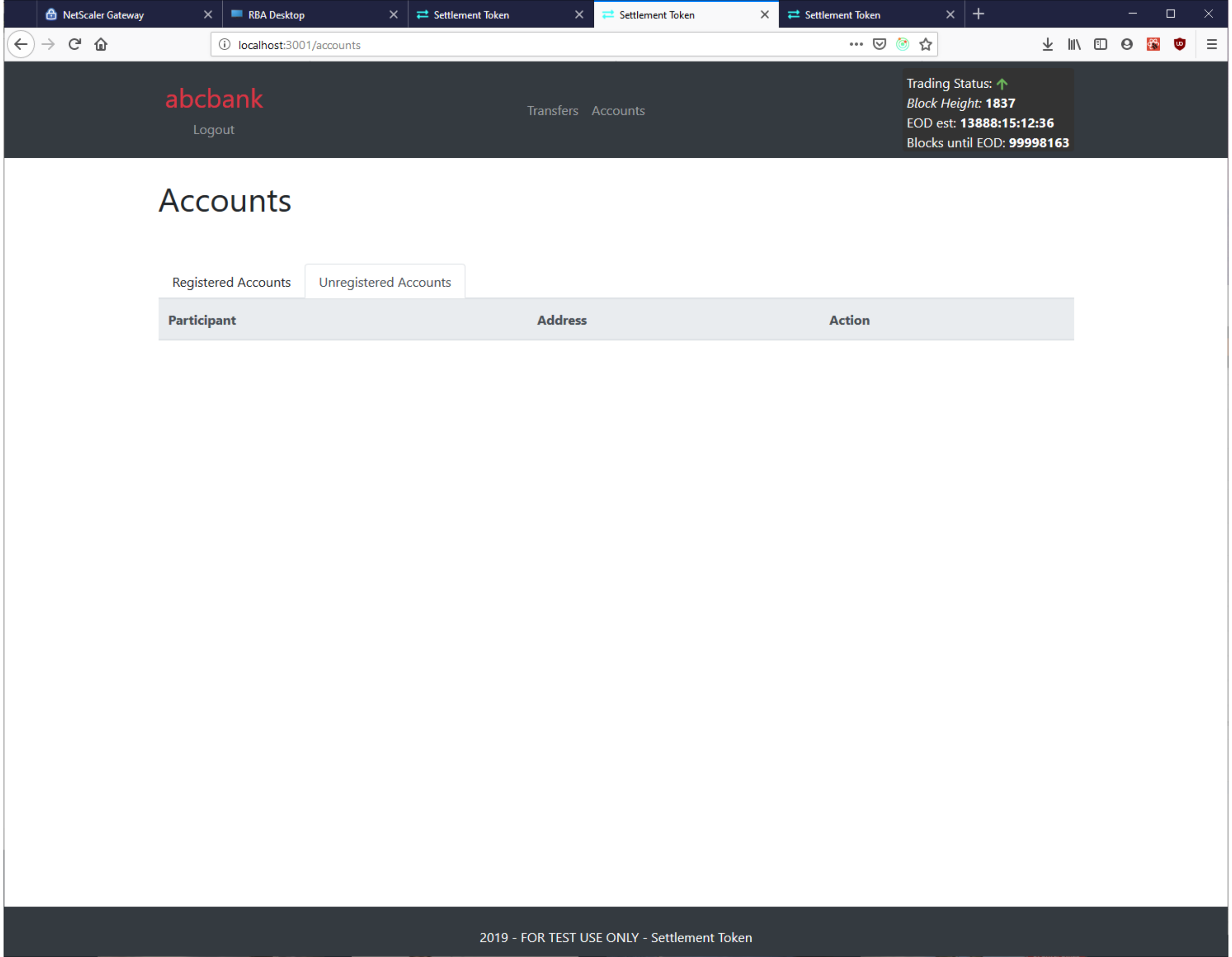


Trading Status: ↑
Block Height: **1828**
EOD est: **13888:15:14:24**
Blocks until EOD: **99998172**

Accounts

Participant	Address	Action
abcbank	0x713713441Fe7cb2480A47E44AA5cFa87Ea675D2F	Request

2019 - FOR TEST USE ONLY - Settlement Token



Trading Status: ↑

Block Height: **1837**

EOD est: **13888:15:12:36**

Blocks until EOD: **99998163**

Accounts

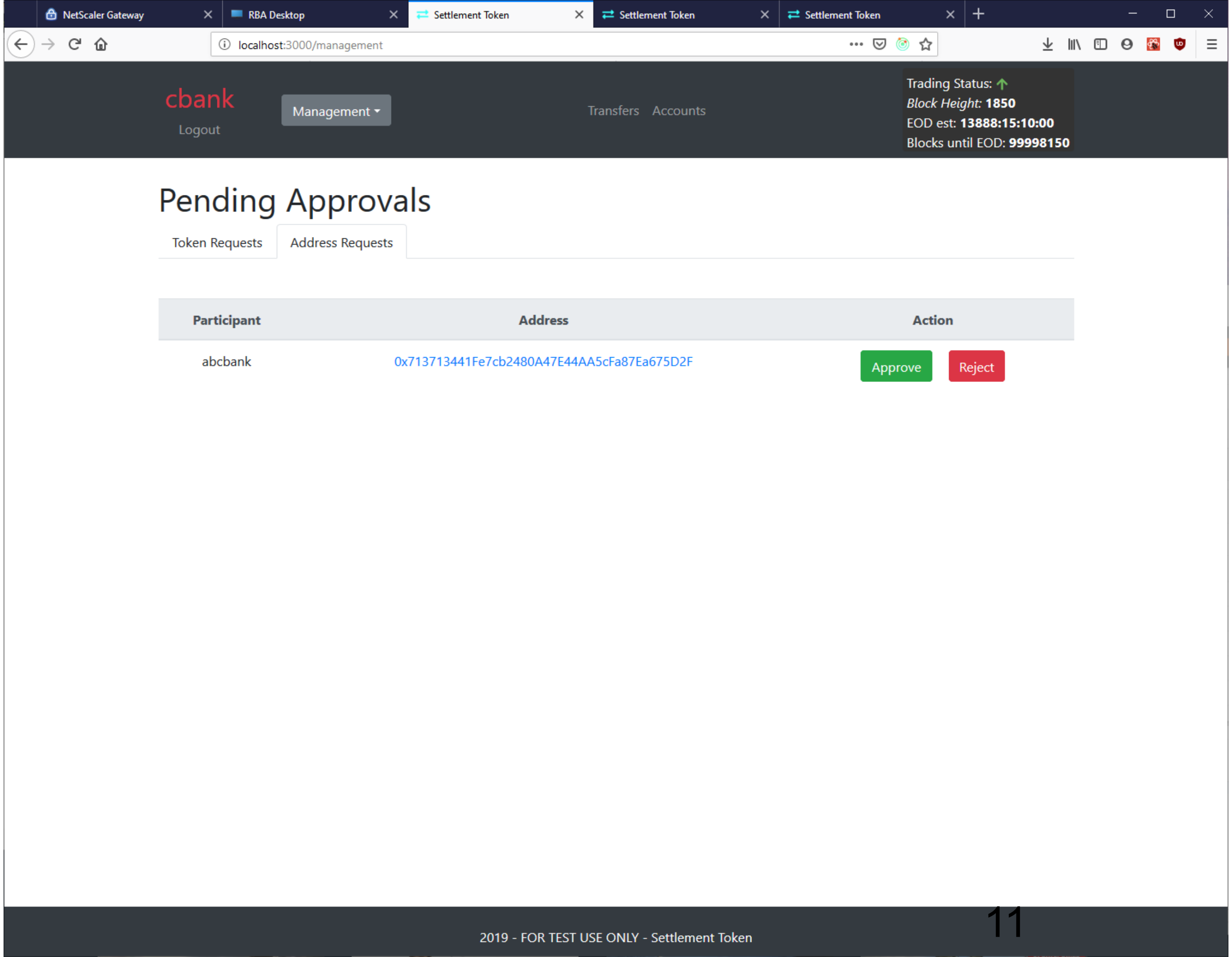
Registered Accounts | Unregistered Accounts

Participant	Address	Action

2019 - FOR TEST USE ONLY - Settlement Token

Day 0

Central Bank approves the account request

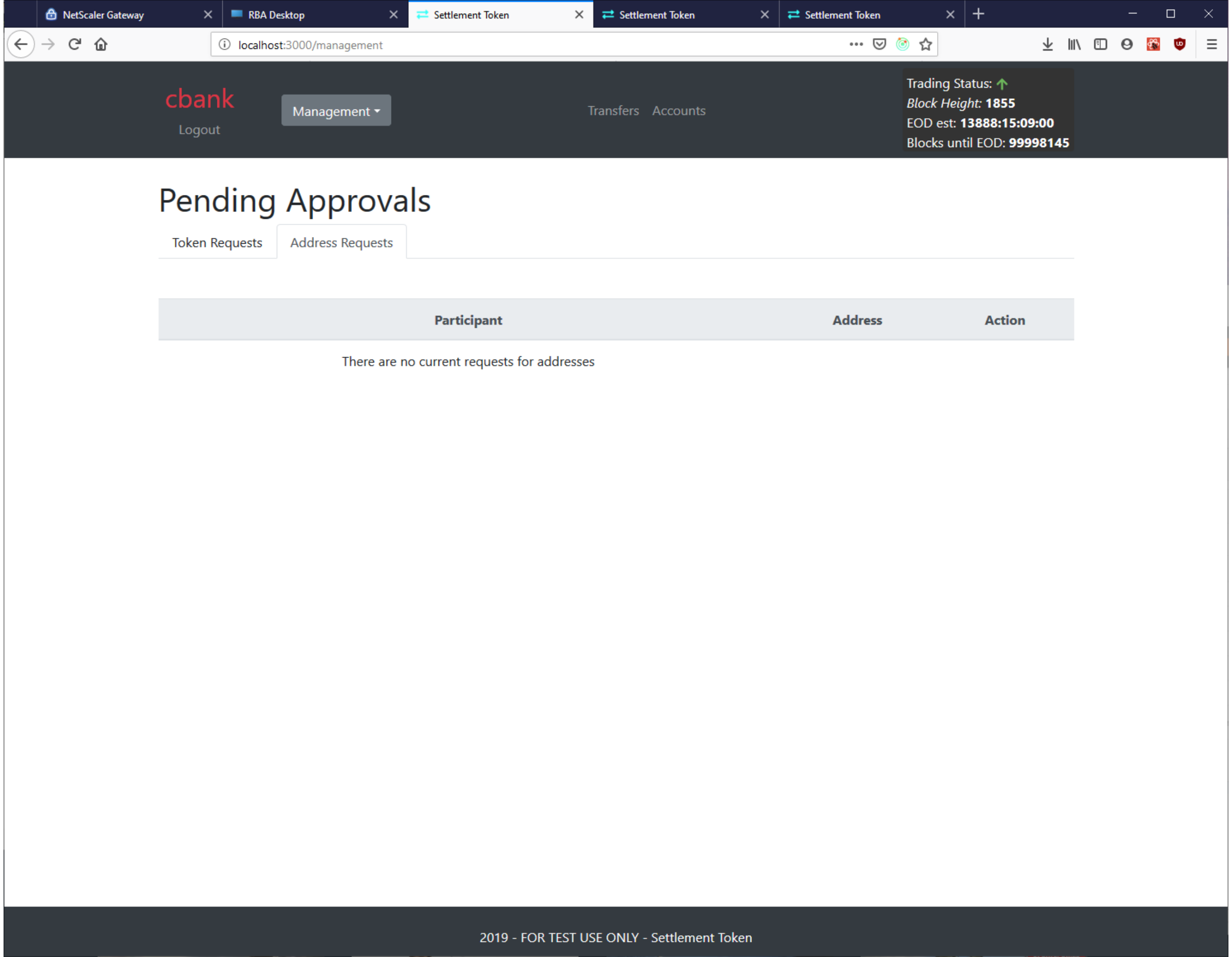


Trading Status: ↑
Block Height: **1850**
EOD est: **13888:15:10:00**
Blocks until EOD: **99998150**

Pending Approvals

Participant	Address	Action
abcbank	0x713713441Fe7cb2480A47E44AA5cFa87Ea675D2F	Approve Reject

2019 - FOR TEST USE ONLY - Settlement Token

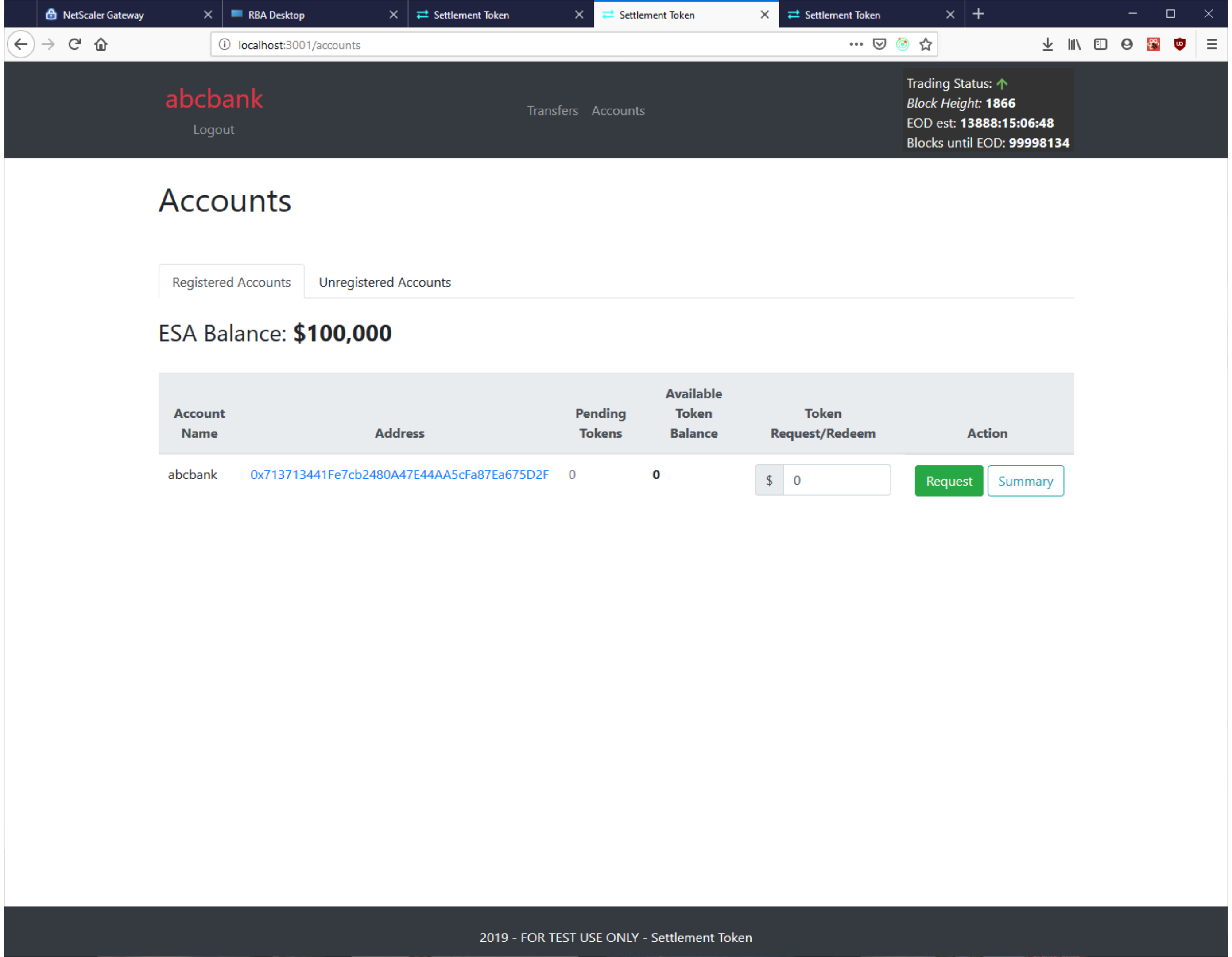


Trading Status: ↑
Block Height: **1855**
EOD est: **13888:15:09:00**
Blocks until EOD: **99998145**

Pending Approvals

Participant	Address	Action
There are no current requests for addresses		

2019 - FOR TEST USE ONLY - Settlement Token



abcbank

Logout

Transfers Accounts

Trading Status: ↑
Block Height: **1866**
EOD est: **13888:15:06:48**
Blocks until EOD: **99998134**

Accounts

Registered Accounts | Unregistered Accounts

ESA Balance: **$100,000**

Account Name	Address	Pending Tokens	Available Token Balance	Token Request/Redeem	Action
abcbank	0x713713441Fe7cb2480A47E44AA5cFa87Ea675D2F	0	**0**	$ 0	Request Summary

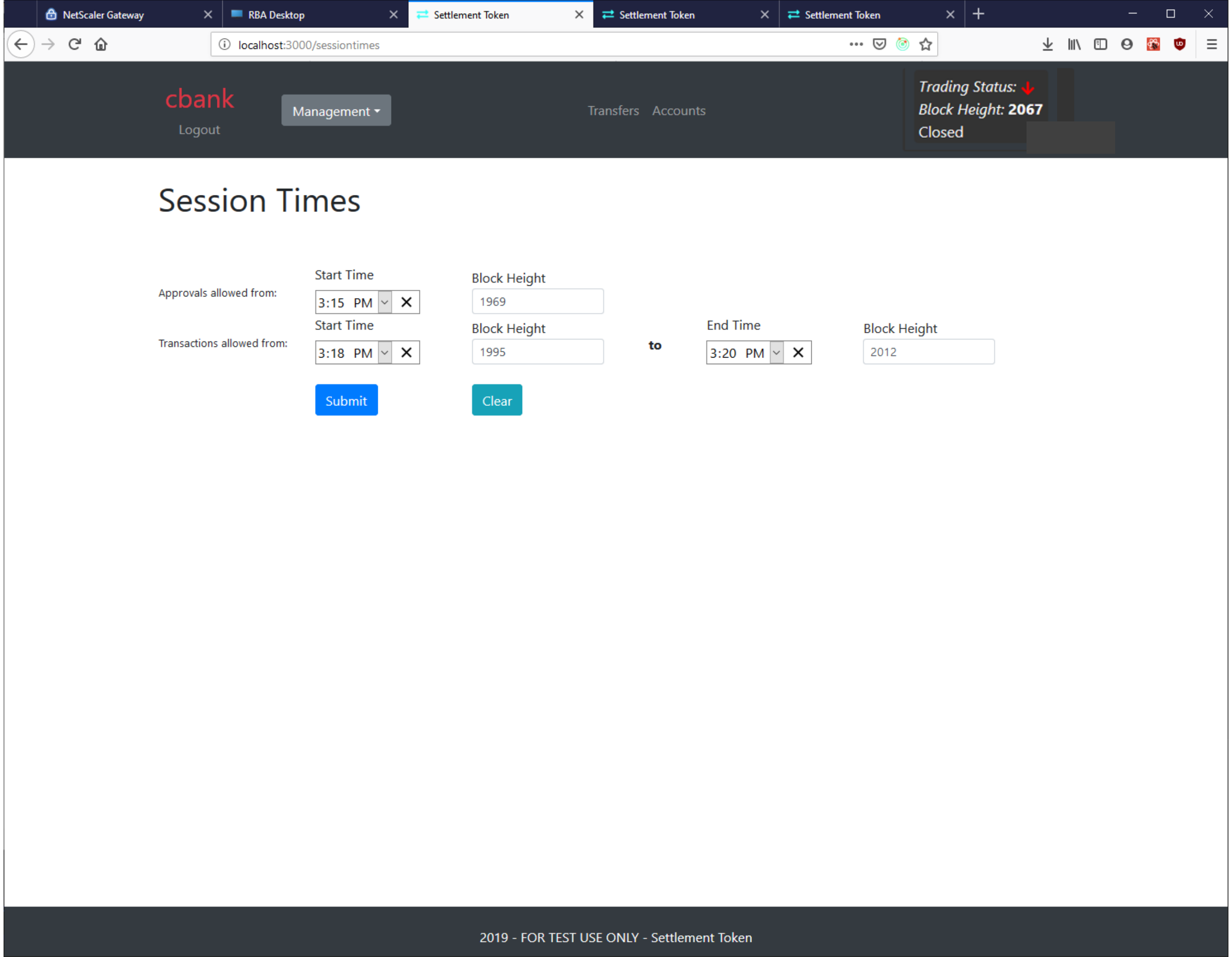
2019 - FOR TEST USE ONLY - Settlement Token

Before start of Day 1 trading

Setting times and approving funds

Before start of Day 1 trading

Central Bank sets times for approvals, SOD and EOD trading

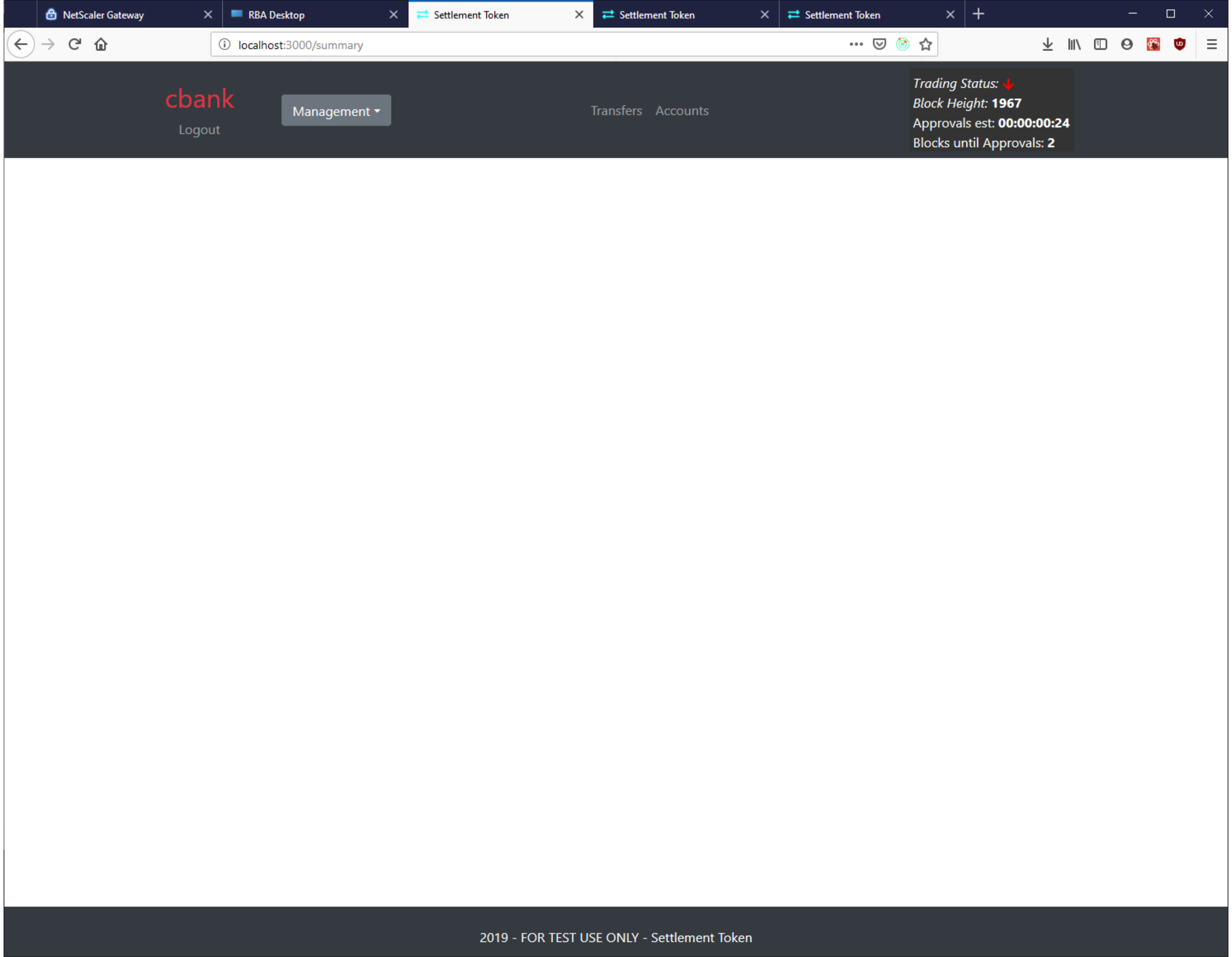


Trading Status: ↓
Block Height: **2067**
Closed

Session Times

	Start Time	Block Height		End Time	Block Height
Approvals allowed from:	3:15 PM	1969			
Transactions allowed from:	3:18 PM	1995	to	3:20 PM	2012

2019 - FOR TEST USE ONLY - Settlement Token



Trading Status: ↓

Block Height: **1967**

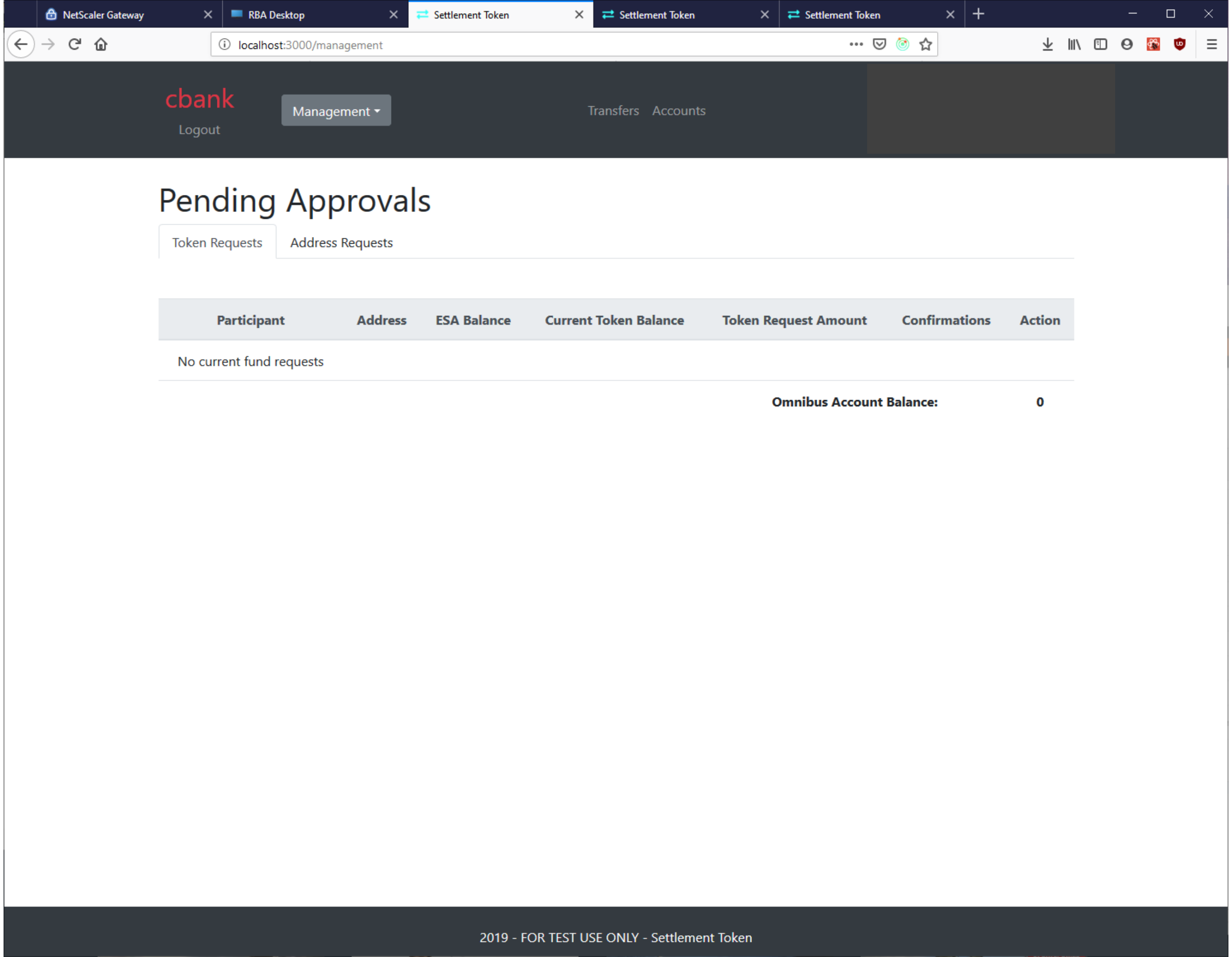
Approvals est: **00:00:00:24**

Blocks until Approvals: **2**

2019 - FOR TEST USE ONLY - Settlement Token

Before start of Day 1 trading

ABC Bank requests tokens before SOD trading

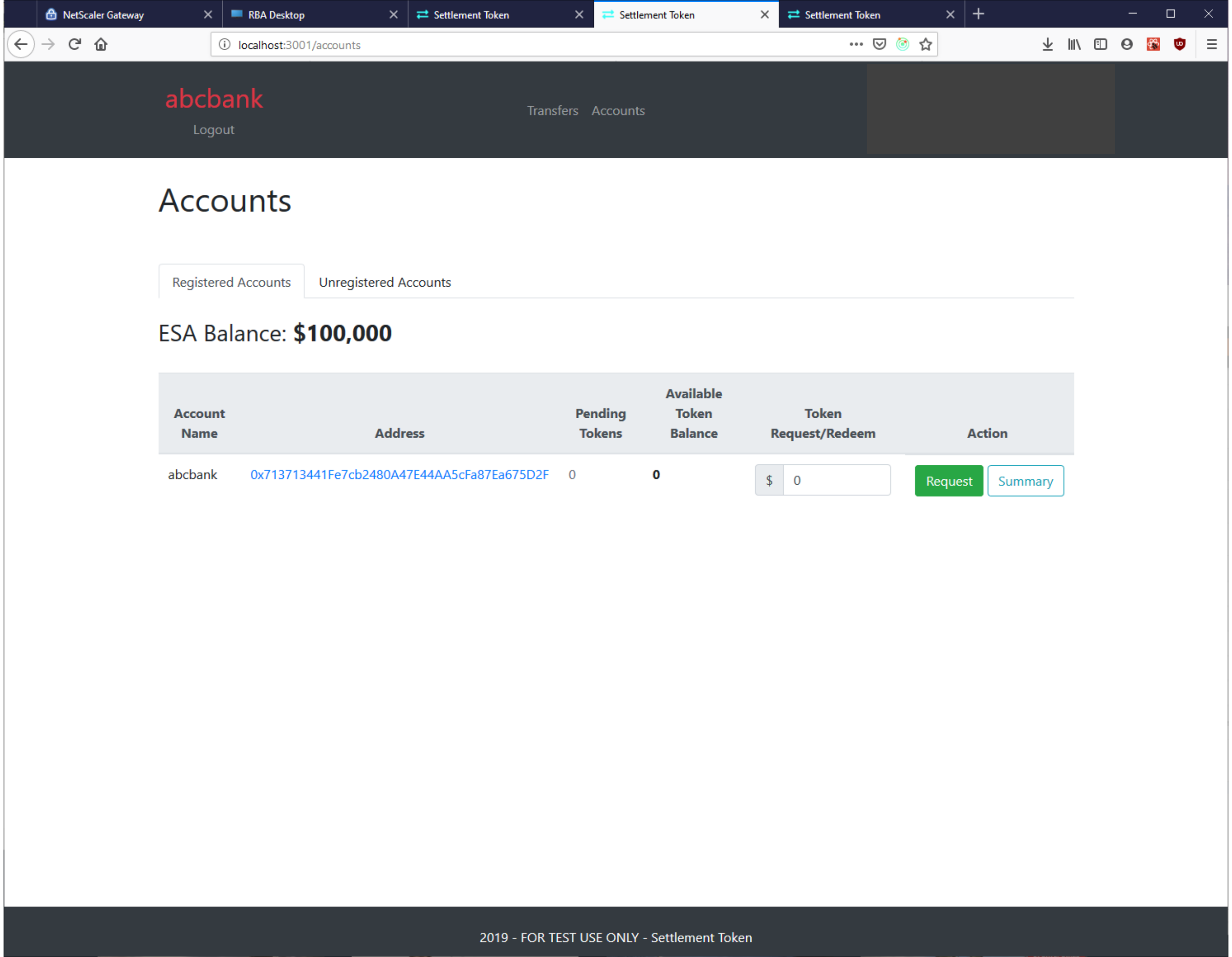


[redacted]

Pending Approvals

Participant	Address	ESA Balance	Current Token Balance	Token Request Amount	Confirmations	Action
No current fund requests						
				Omnibus Account Balance:		**0**

2019 - FOR TEST USE ONLY - Settlement Token



abcbank

Logout

Transfers Accounts

[redacted]

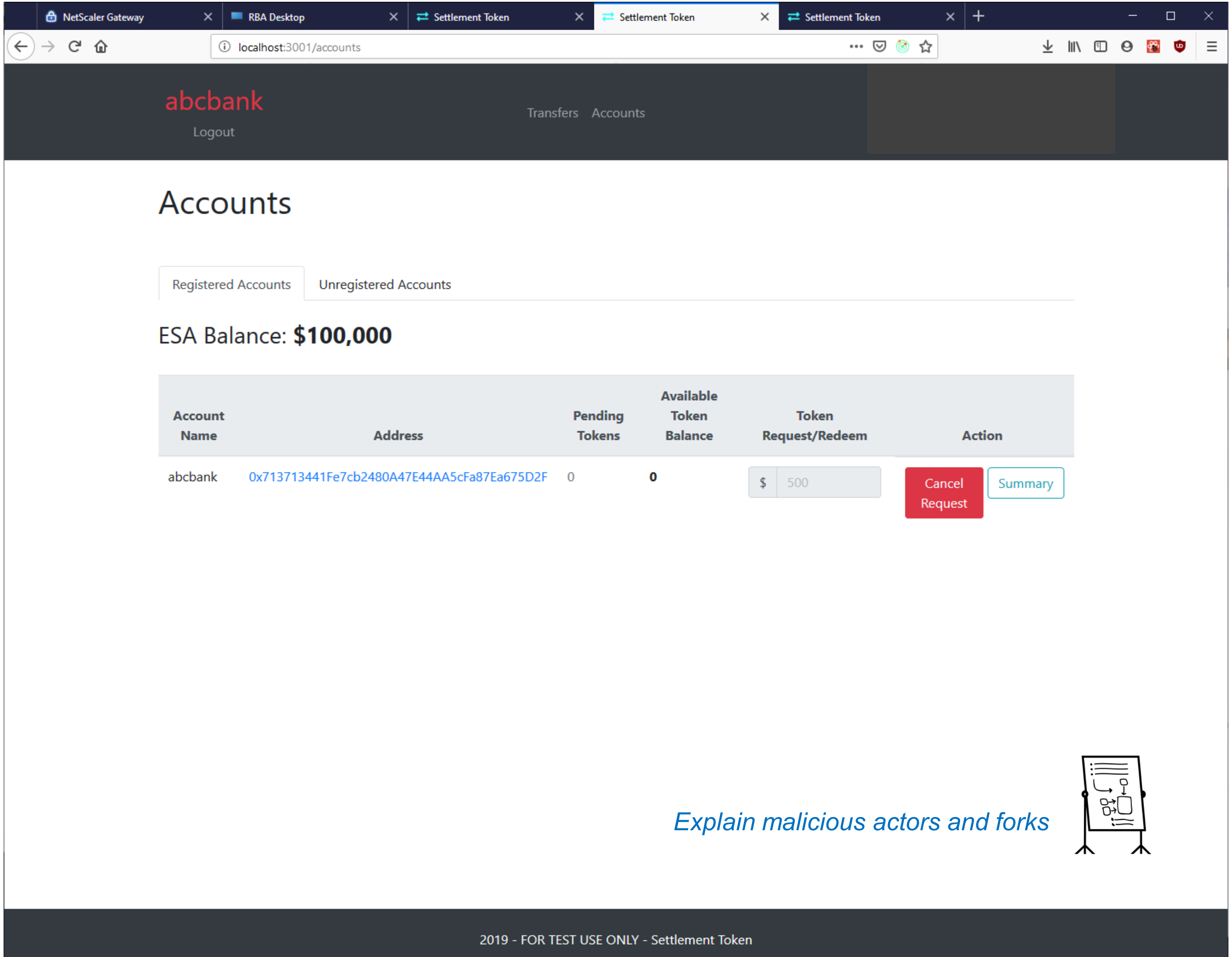
Accounts

Registered Accounts | Unregistered Accounts

ESA Balance: **$100,000**

Account Name	Address	Pending Tokens	Available Token Balance	Token Request/Redeem	Action
abcbank	0x713713441Fe7cb2480A47E44AA5cFa87Ea675D2F	0	**0**	$ 0	Request Summary

2019 - FOR TEST USE ONLY - Settlement Token



Accounts

ESA Balance: **$100,000**

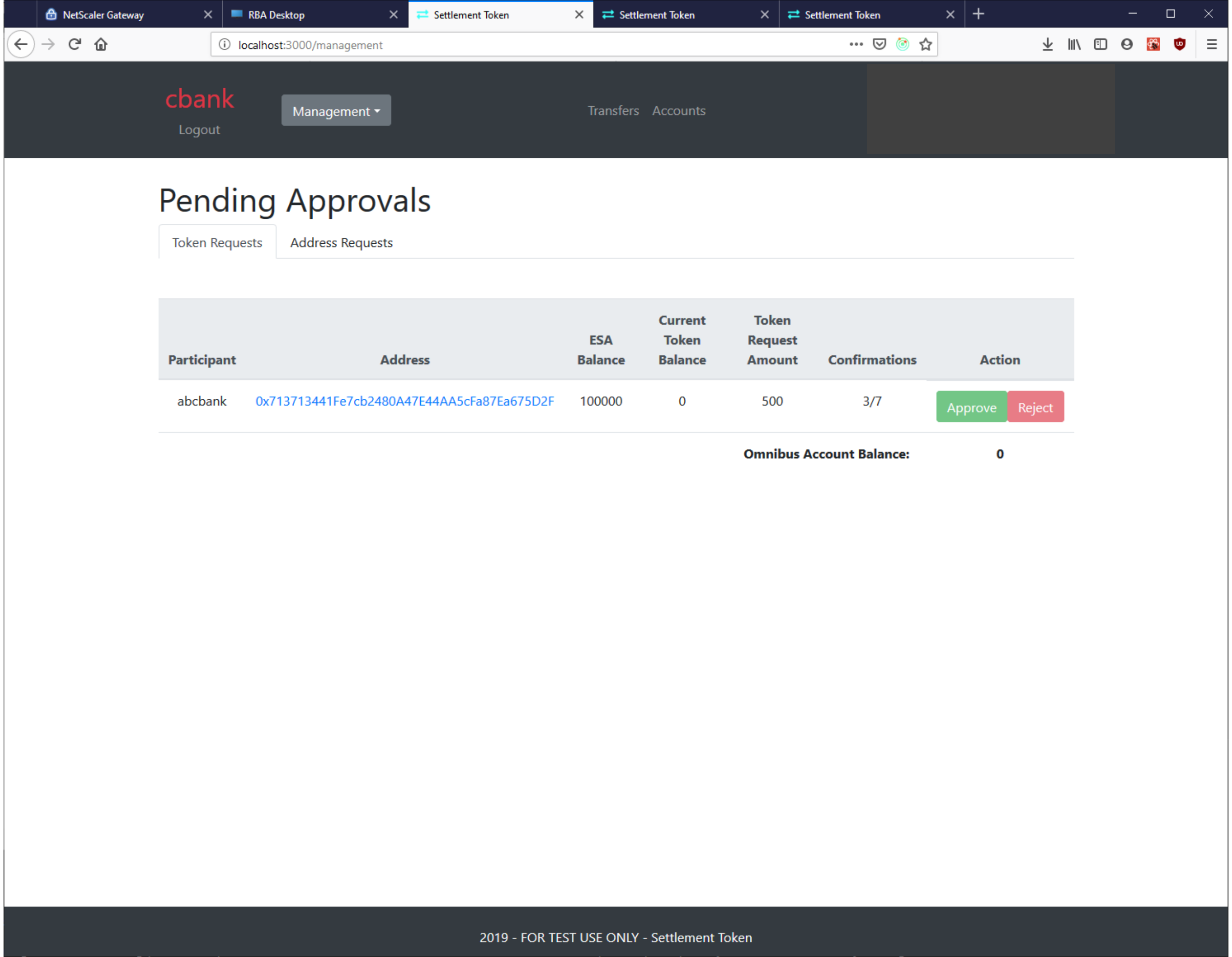
Account Name	Address	Pending Tokens	Available Token Balance	Token Request/Redeem	Action
abcbank	0x713713441Fe7cb2480A47E44AA5cFa87Ea675D2F	0	**0**	$ 500	Cancel Request Summary

Explain malicious actors and forks

2019 - FOR TEST USE ONLY - Settlement Token

Before start of Day 1 trading

Central Bank approves ABC Bank token request before SOD training



cbank

Logout

Management ▾

Transfers Accounts

[redacted]

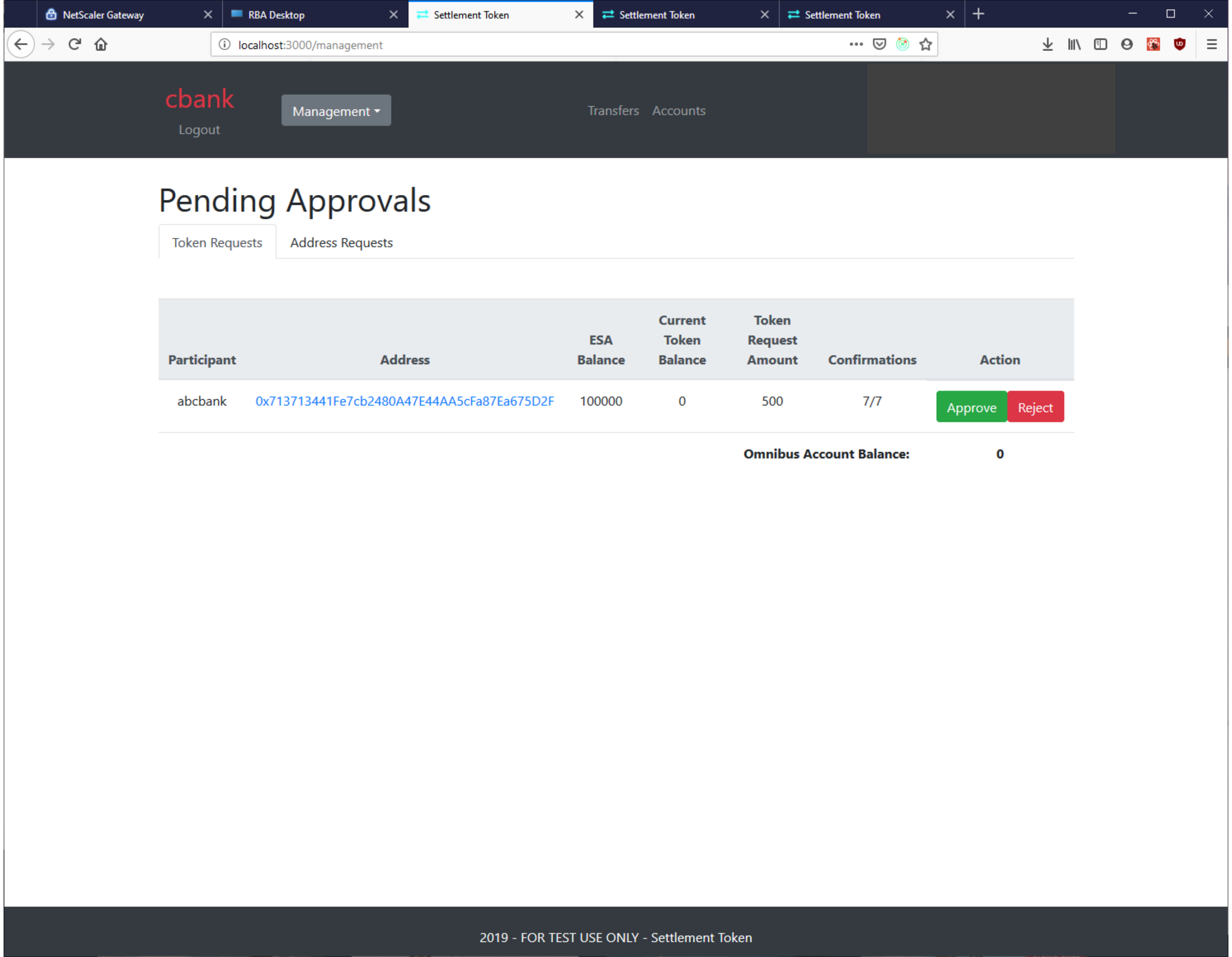
Pending Approvals

Token Requests | Address Requests

Participant	Address	ESA Balance	Current Token Balance	Token Request Amount	Confirmations	Action
abcbank	0x713713441Fe7cb2480A47E44AA5cFa87Ea675D2F	100000	0	500	3/7	Approve Reject

Omnibus Account Balance: **0**

2019 - FOR TEST USE ONLY - Settlement Token



[redacted]

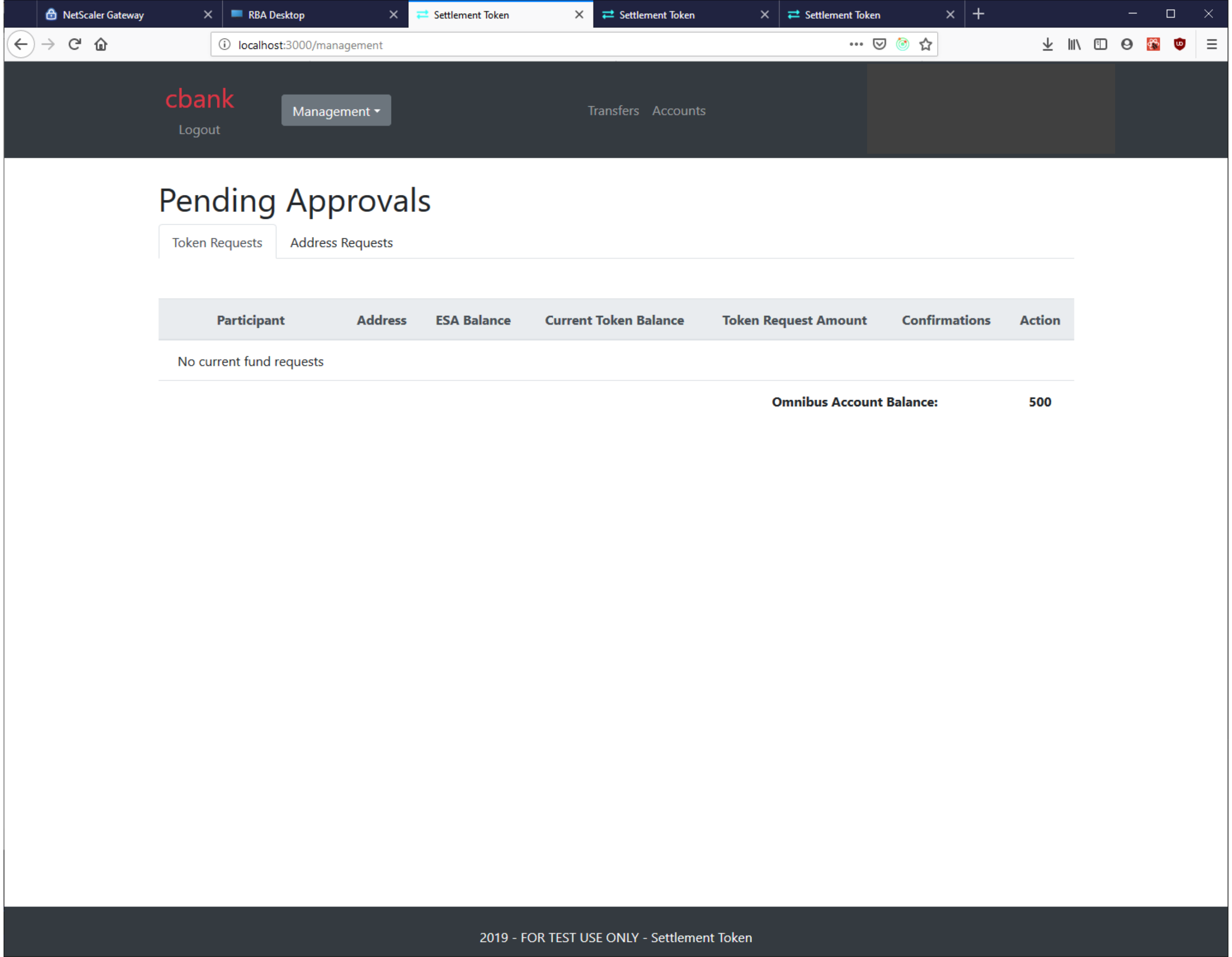
Pending Approvals

Token Requests | Address Requests

Participant	Address	ESA Balance	Current Token Balance	Token Request Amount	Confirmations	Action
abcbank	0x713713441Fe7cb2480A47E44AA5cFa87Ea675D2F	100000	0	500	7/7	Approve Reject

Omnibus Account Balance: **0**

2019 - FOR TEST USE ONLY - Settlement Token



[redacted]

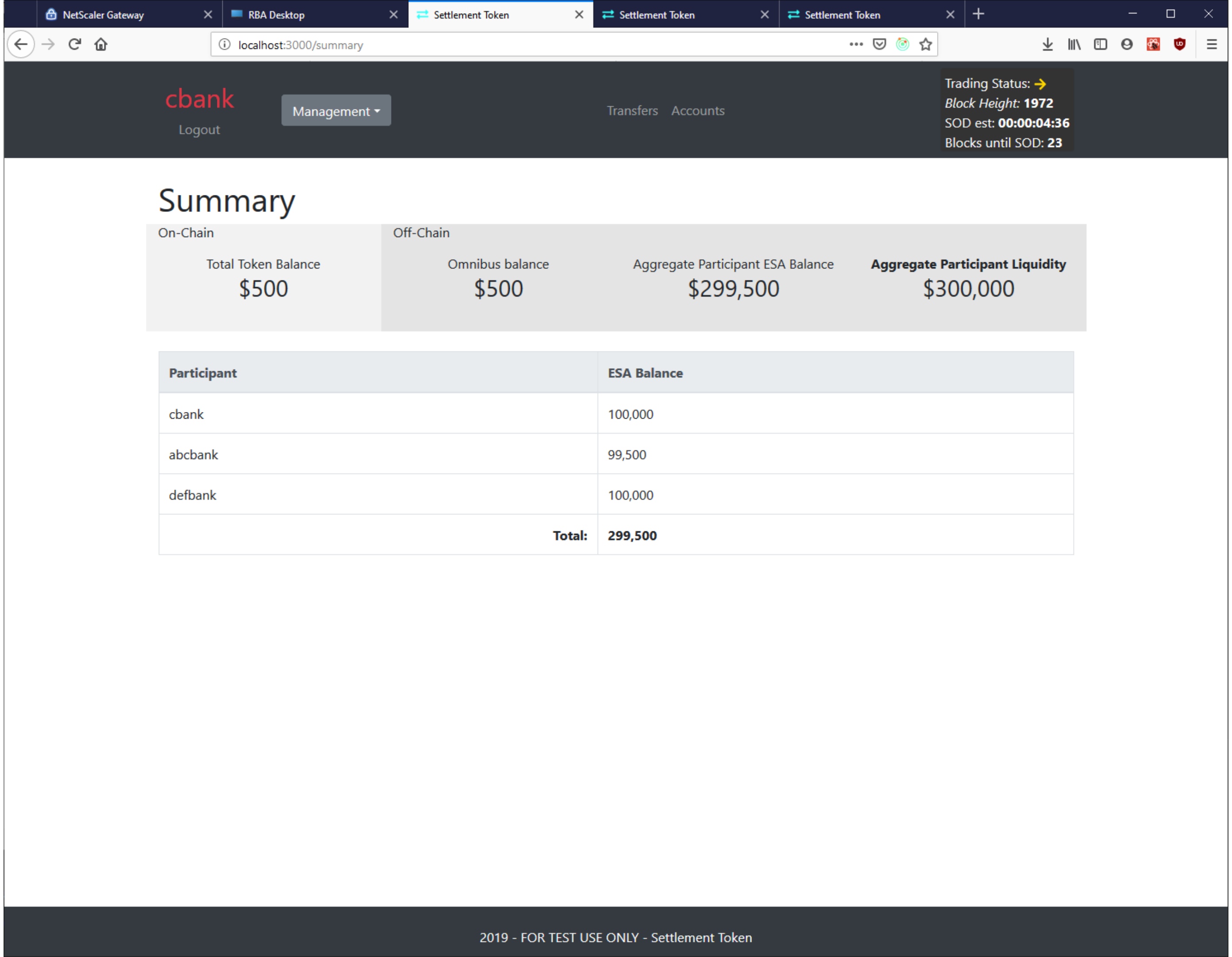
Pending Approvals

Token Requests | Address Requests

Participant	Address	ESA Balance	Current Token Balance	Token Request Amount	Confirmations	Action
No current fund requests						

Omnibus Account Balance: **500**

2019 - FOR TEST USE ONLY - Settlement Token



Trading Status:

Block Height: **1972**

SOD est: **00:00:04:36**

Blocks until SOD: **23**

Summary

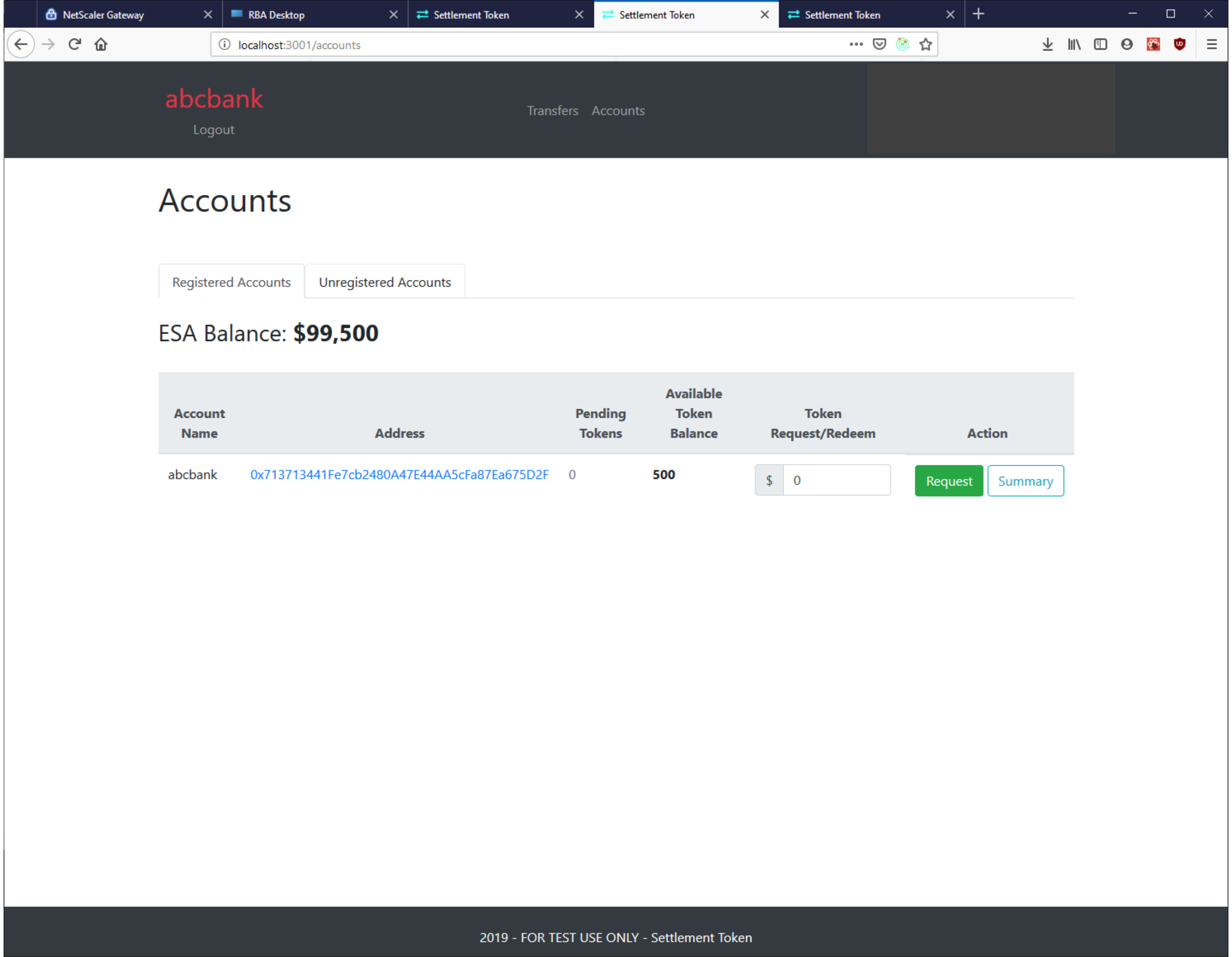
On-Chain	Off-Chain		
Total Token Balance	Omnibus balance	Aggregate Participant ESA Balance	**Aggregate Participant Liquidity**
$500	$500	$299,500	$300,000

Participant	ESA Balance
cbank	100,000
abcbank	99,500
defbank	100,000
Total:	**299,500**

2019 - FOR TEST USE ONLY - Settlement Token

Before start of Day 1 trading

ABC Bank views approved token balance before SOD training



abcbank

Logout

Transfers Accounts

[redacted]

Accounts

Registered Accounts | Unregistered Accounts

ESA Balance: **$99,500**

Account Name	Address	Pending Tokens	Available Token Balance	Token Request/Redeem	Action
abcbank	0x713713441Fe7cb2480A47E44AA5cFa87Ea675D2F	0	**500**	$ 0	Request Summary

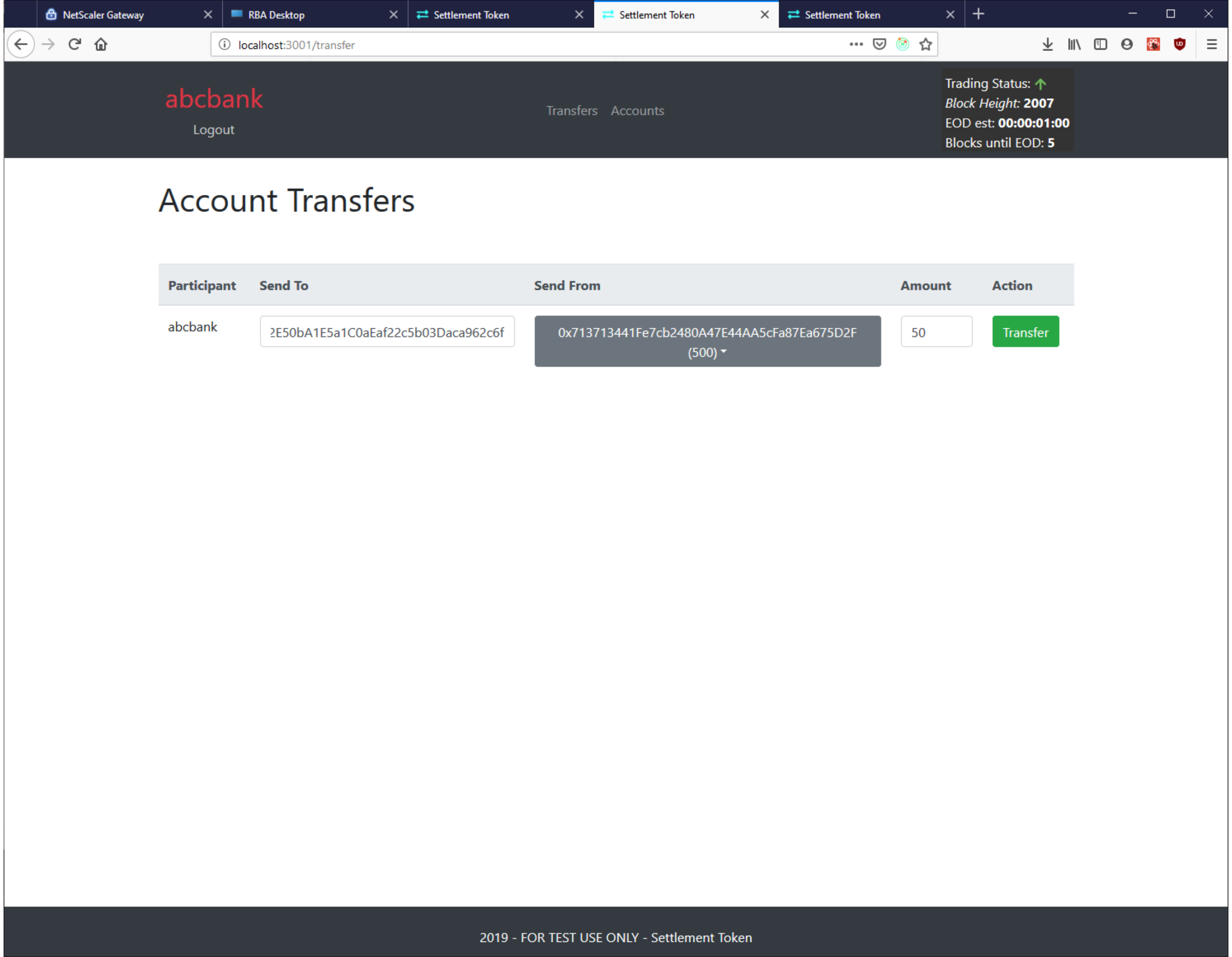
2019 - FOR TEST USE ONLY - Settlement Token

Day 1

Transferring funds and end-of-day

Day 1

ABC Bank transfers tokenised funds to DEF Bank



Trading Status:

Block Height: **2007**

EOD est: **00:00:01:00**

Blocks until EOD: **5**

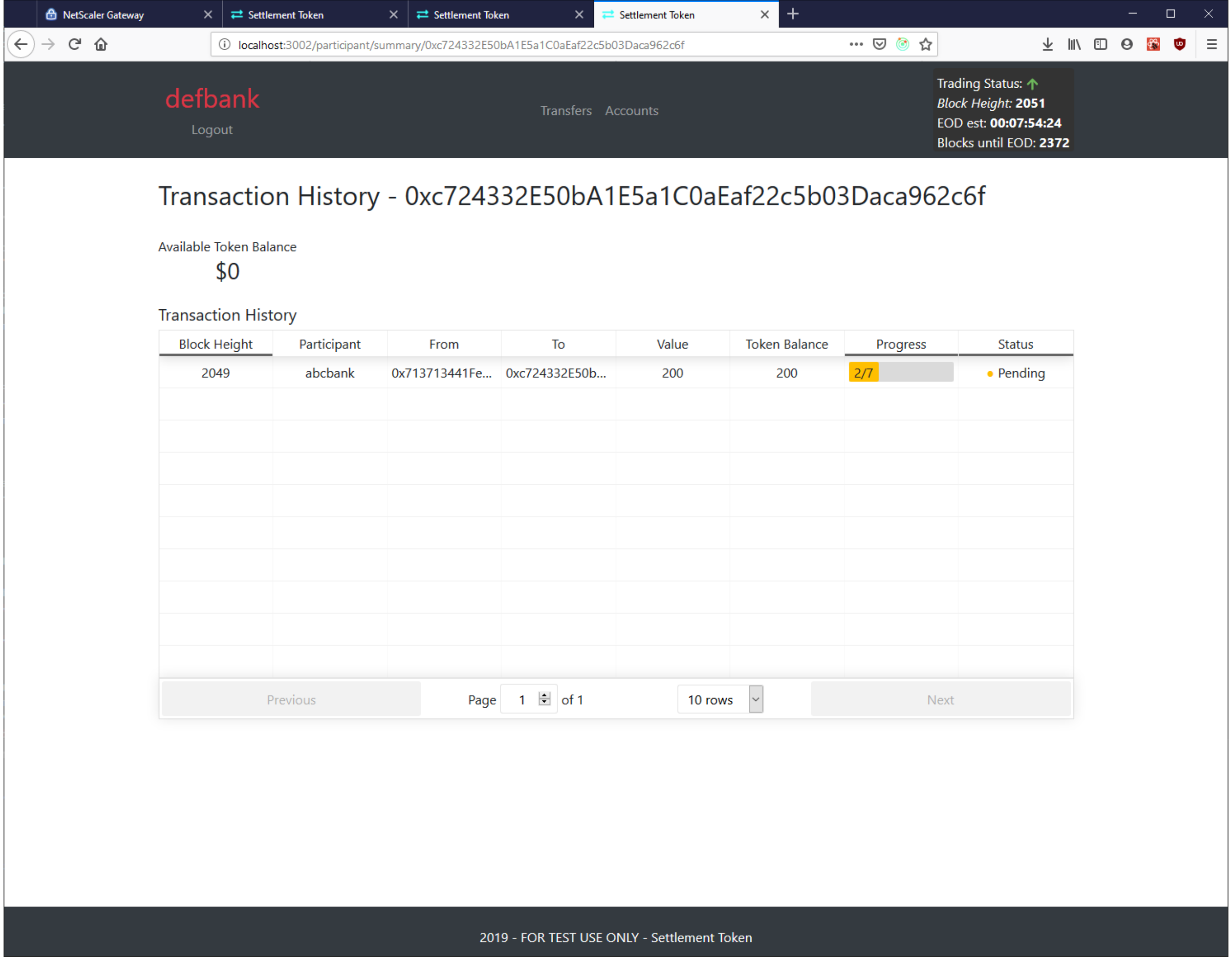
Account Transfers

Participant	Send To	Send From	Amount	Action
abcbank	?E50bA1E5a1C0aEaf22c5b03Daca962c6f	0x713713441Fe7cb2480A47E44AA5cFa87Ea675D2F (500) ▾	50	Transfer

2019 - FOR TEST USE ONLY - Settlement Token

Day 1

DEF Bank receives tokenised funds from ABC Bank



Trading Status: ↑
Block Height: **2051**
EOD est: **00:07:54:24**
Blocks until EOD: **2372**

Transaction History - 0xc724332E50bA1E5a1C0aEaf22c5b03Daca962c6f

Available Token Balance

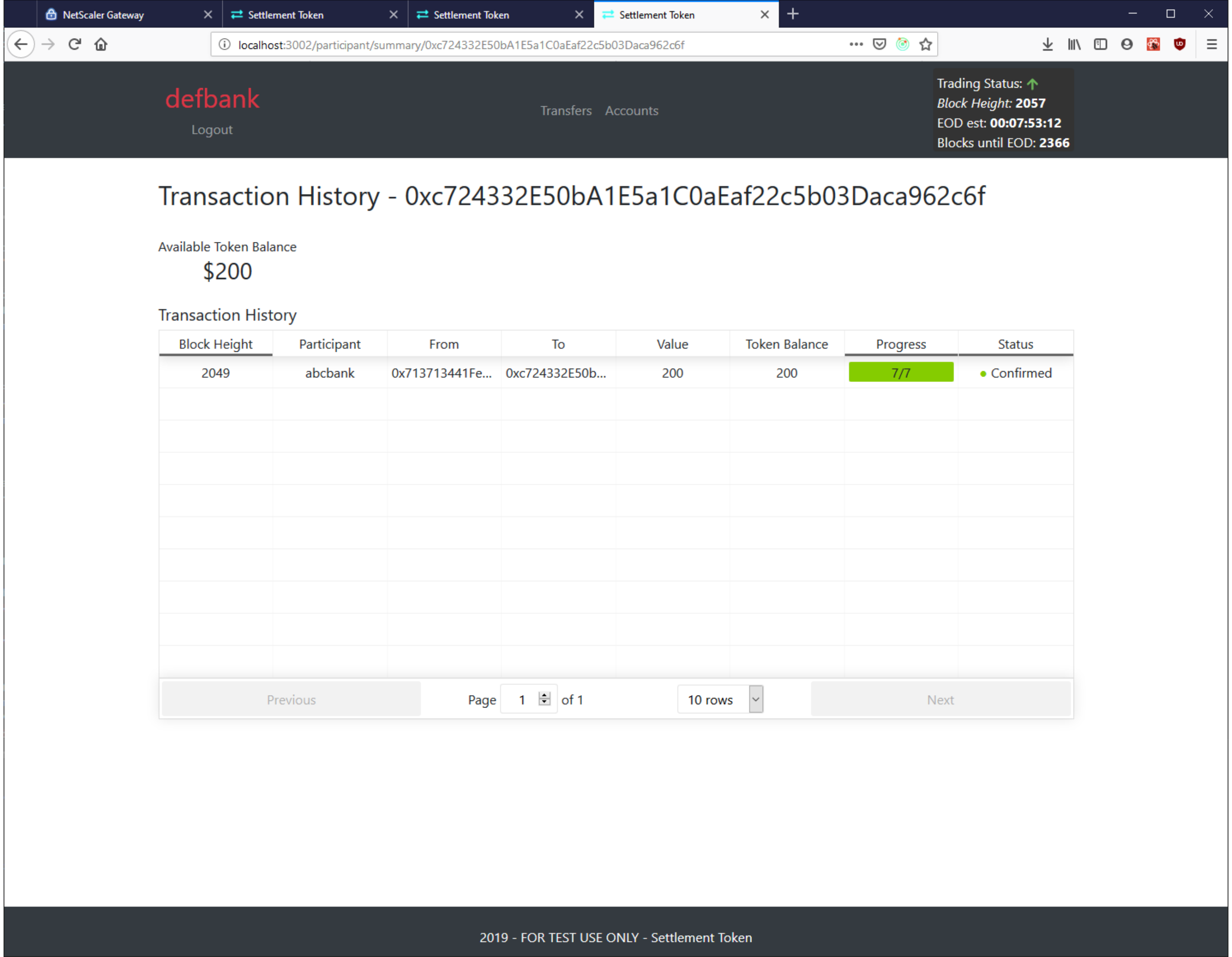
$0

Transaction History

Block Height	Participant	From	To	Value	Token Balance	Progress	Status
2049	abcbank	0x713713441Fe...	0xc724332E50b...	200	200	2/7	● Pending

Page 1 of 1 | 10 rows

2019 - FOR TEST USE ONLY - Settlement Token


NetScaler Gateway
Settlement Token
Settlement Token
Settlement Token
localhost:3002/participant/summary/0xc724332E50bA1E5a1C0aEaf22c5b03Daca962c6f

defbank

Logout

Transfers Accounts

Trading Status: ↑
Block Height: **2057**
EOD est: **00:07:53:12**
Blocks until EOD: **2366**

Transaction History - 0xc724332E50bA1E5a1C0aEaf22c5b03Daca962c6f

Available Token Balance

$200

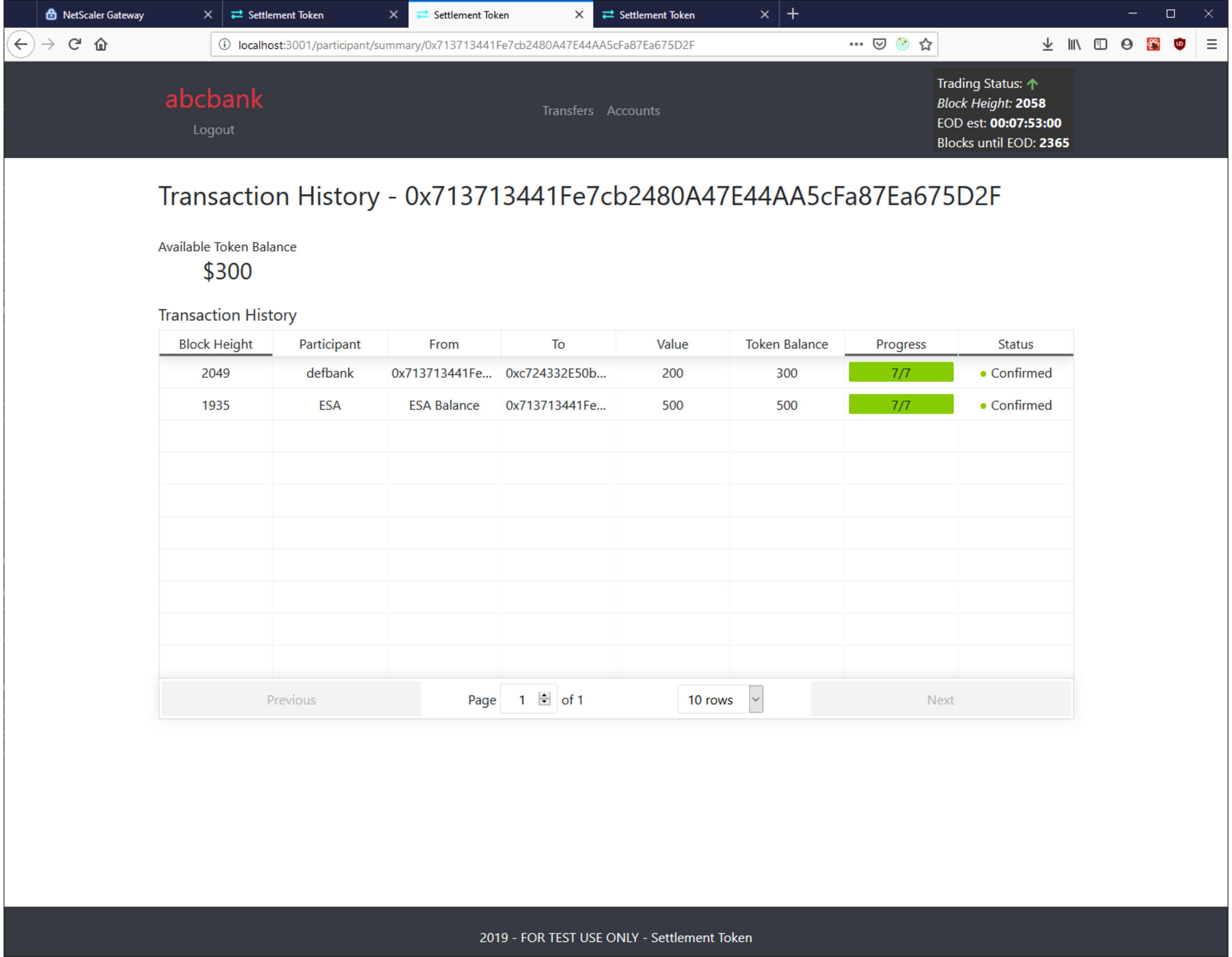
Transaction History

Block Height	Participant	From	To	Value	Token Balance	Progress	Status
2049	abcbank	0x713713441Fe...	0xc724332E50b...	200	200	7/7	● Confirmed

2019 - FOR TEST USE ONLY - Settlement Token

Day 1

ABC Bank confirms its transfer to DEF Bank in the transaction history page


NetScaler Gateway
Settlement Token
Settlement Token
Settlement Token
localhost:3001/participant/summary/0x713713441Fe7cb2480A47E44AA5cFa87Ea675D2F

abcbank

Logout

Transfers Accounts

Trading Status: ↑
Block Height: **2058**
EOD est: **00:07:53:00**
Blocks until EOD: **2365**

Transaction History - 0x713713441Fe7cb2480A47E44AA5cFa87Ea675D2F

Available Token Balance

$300

Transaction History

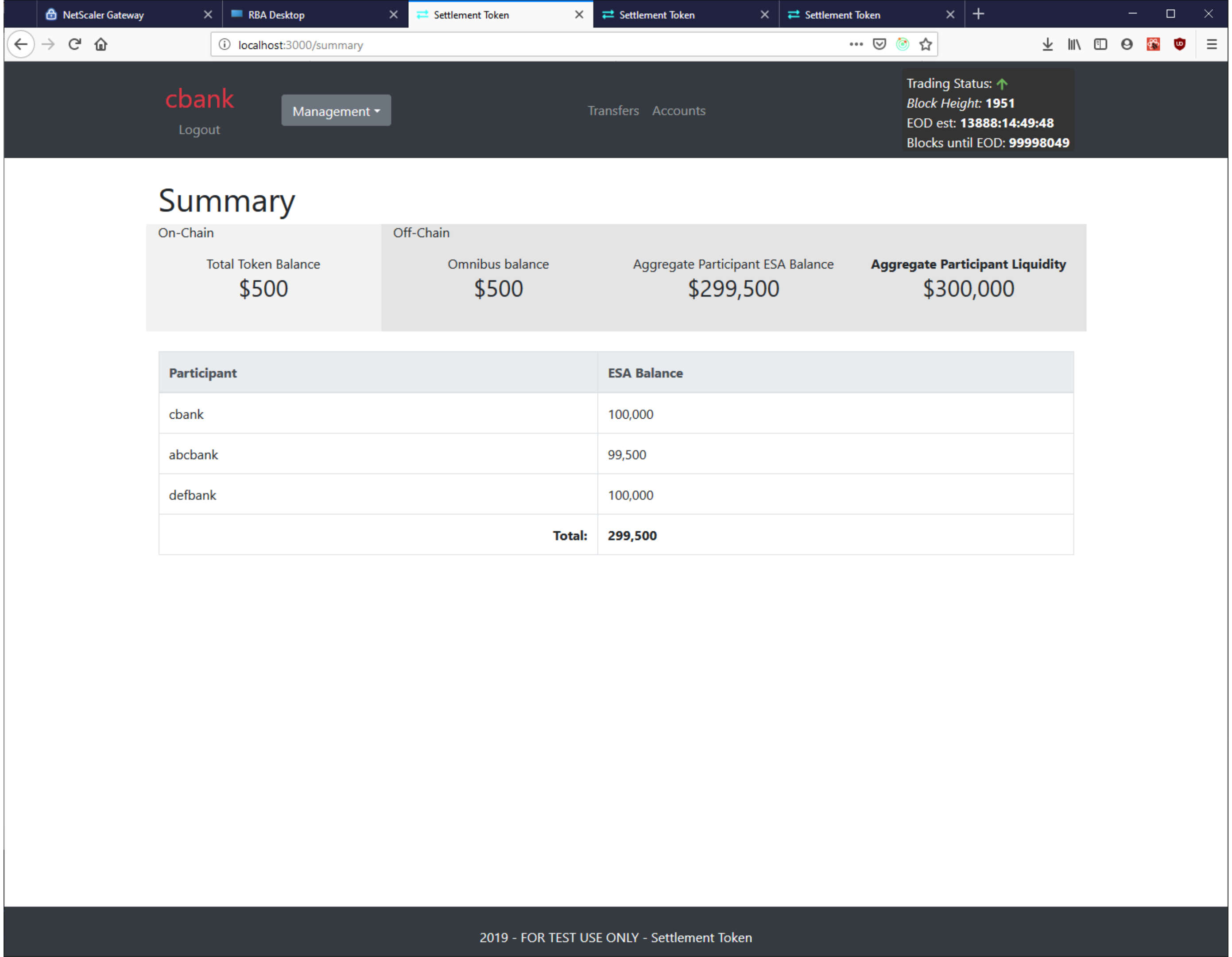
Block Height	Participant	From	To	Value	Token Balance	Progress	Status
2049	defbank	0x713713441Fe...	0xc724332E50b...	200	300	7/7	● Confirmed
1935	ESA	ESA Balance	0x713713441Fe...	500	500	7/7	● Confirmed

Previous Page 1 of 1 10 rows Next

2019 - FOR TEST USE ONLY - Settlement Token

Day 1

Central Bank views system liquidity



Trading Status: ↑
Block Height: **1951**
EOD est: **13888:14:49:48**
Blocks until EOD: **99998049**

Summary

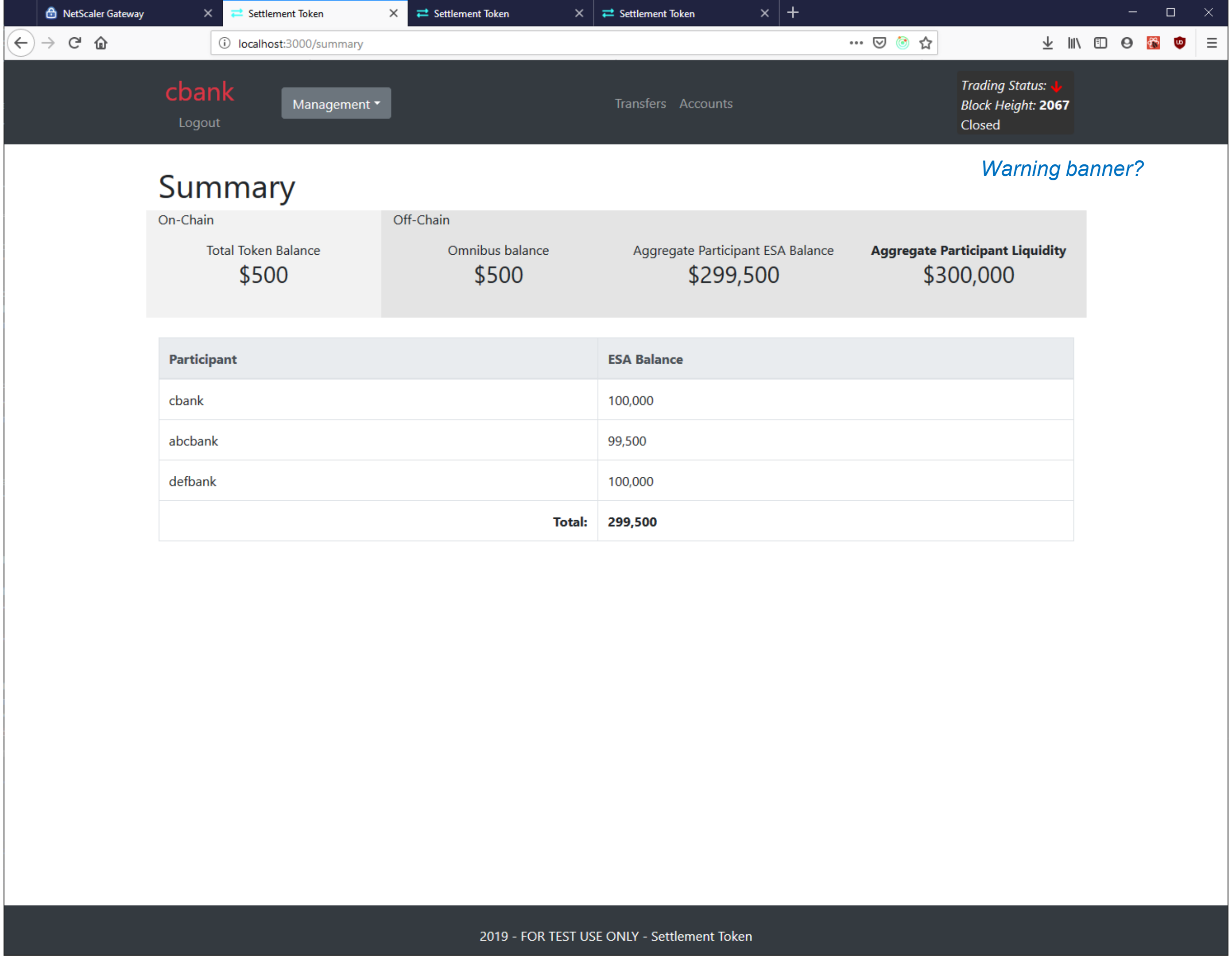
On-Chain	Off-Chain		
Total Token Balance	Omnibus balance	Aggregate Participant ESA Balance	**Aggregate Participant Liquidity**
$500	$500	$299,500	$300,000

Participant	ESA Balance
cbank	100,000
abcbank	99,500
defbank	100,000
Total:	**299,500**

2019 - FOR TEST USE ONLY - Settlement Token

Day 1

Sweep



Trading Status: ↓
Block Height: **2067**
Closed

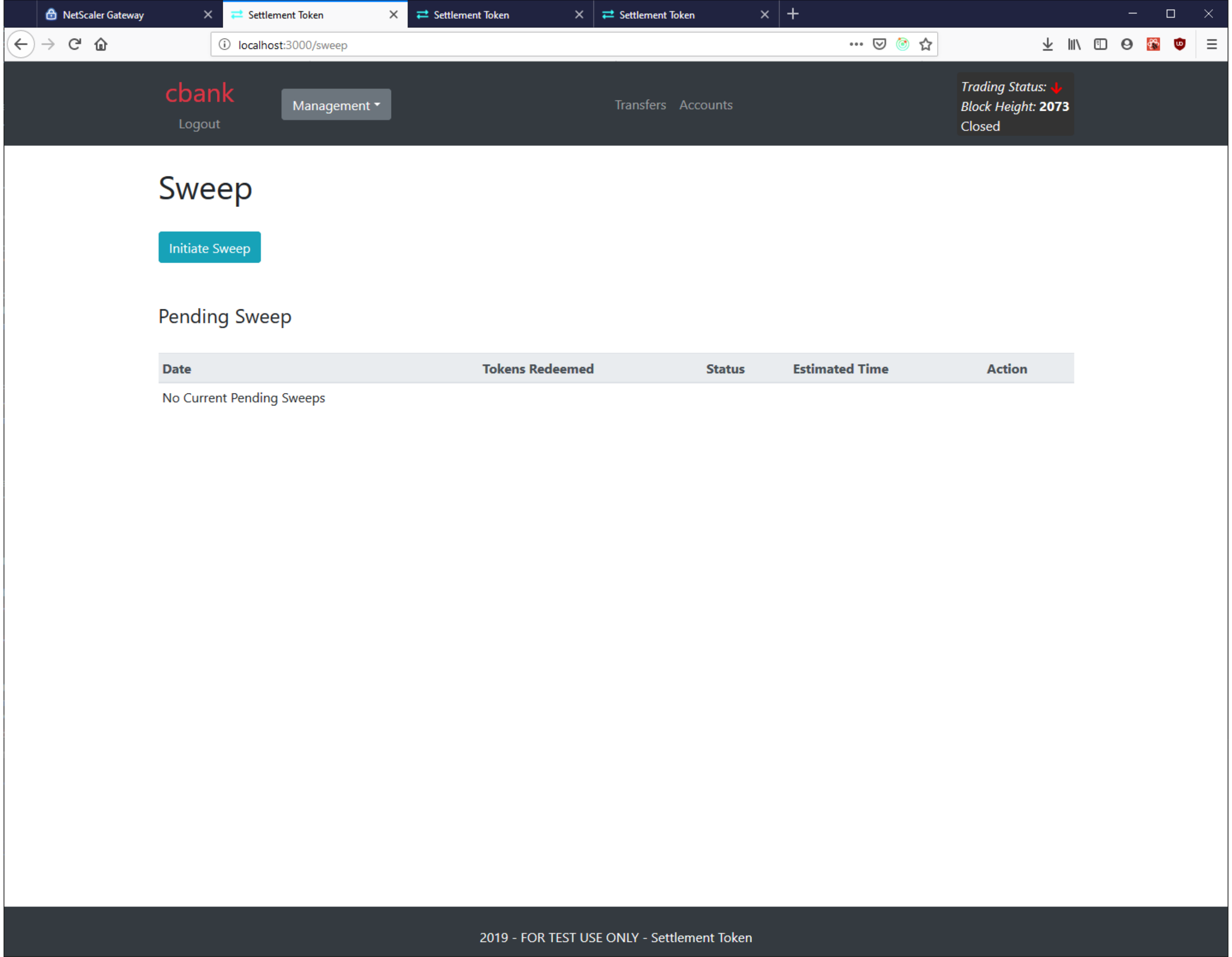
Warning banner?

Summary

On-Chain	Off-Chain		
Total Token Balance	Omnibus balance	Aggregate Participant ESA Balance	**Aggregate Participant Liquidity**
$500	$500	$299,500	$300,000

Participant	ESA Balance
cbank	100,000
abcbank	99,500
defbank	100,000
Total:	**299,500**

2019 - FOR TEST USE ONLY - Settlement Token



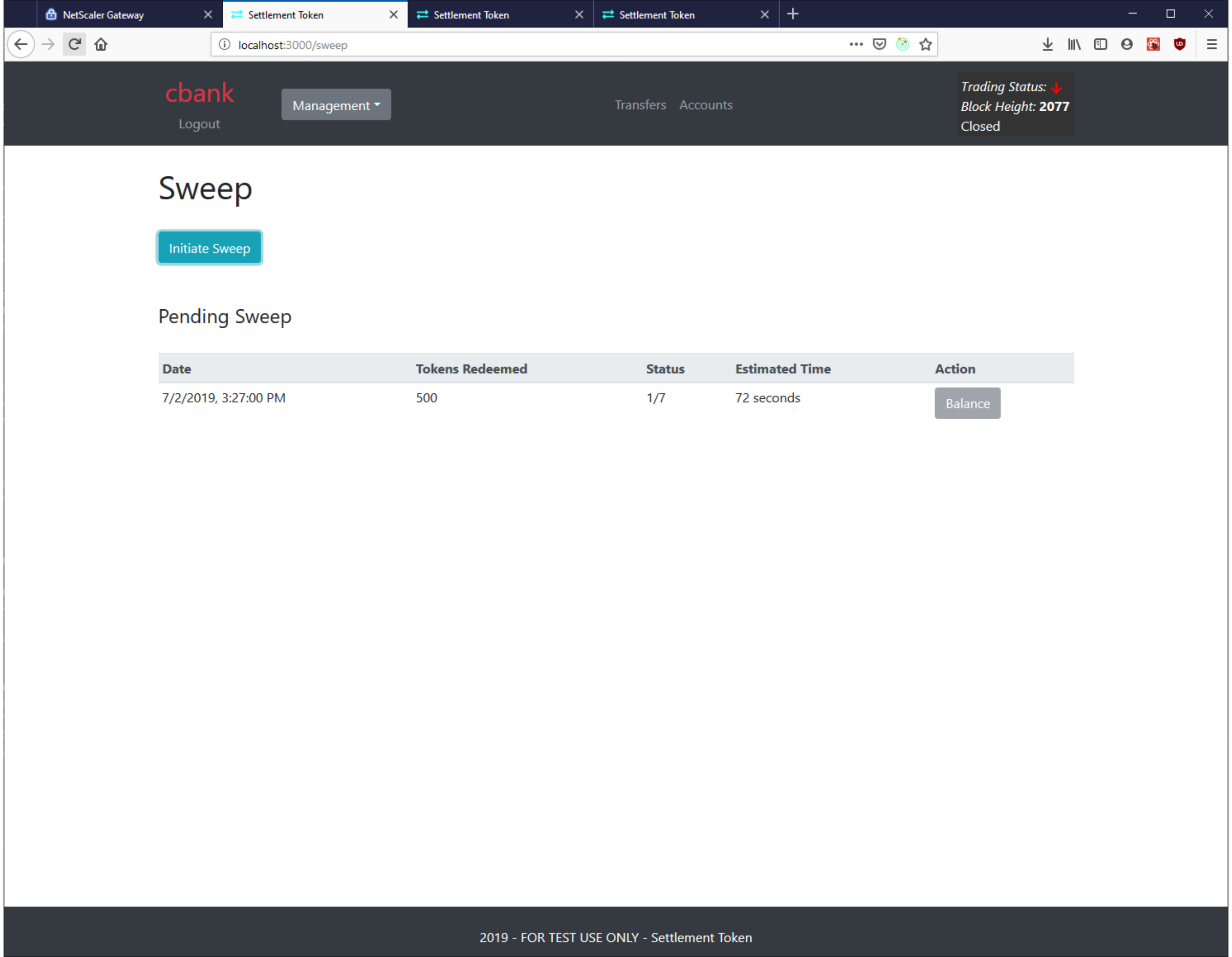
Trading Status: ↓
Block Height: **2073**
Closed

Sweep

Pending Sweep

Date	Tokens Redeemed	Status	Estimated Time	Action
No Current Pending Sweeps				

2019 - FOR TEST USE ONLY - Settlement Token



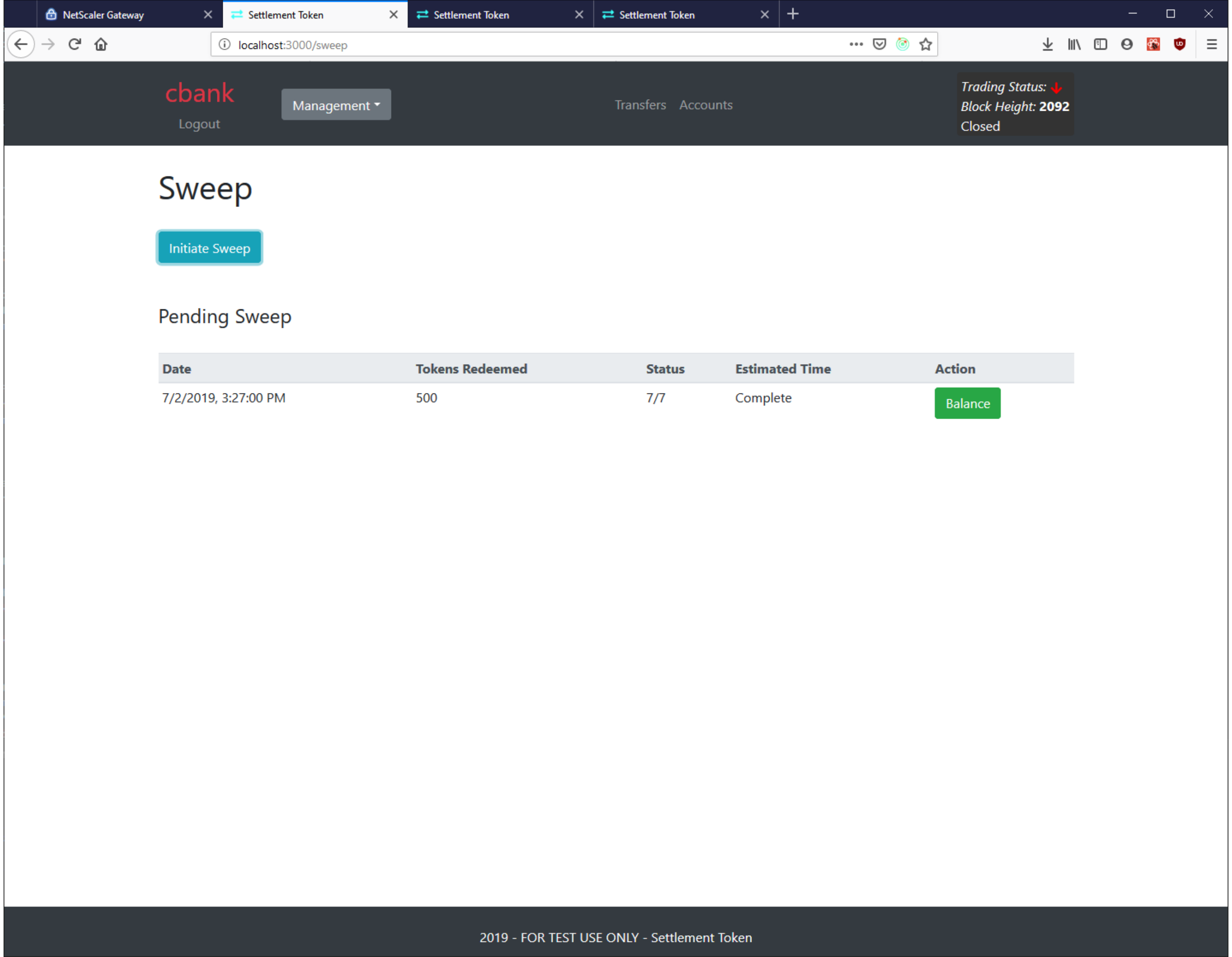
Trading Status: ↓
Block Height: **2077**
Closed

Sweep

Pending Sweep

Date	Tokens Redeemed	Status	Estimated Time	Action
7/2/2019, 3:27:00 PM	500	1/7	72 seconds	Balance

2019 - FOR TEST USE ONLY - Settlement Token



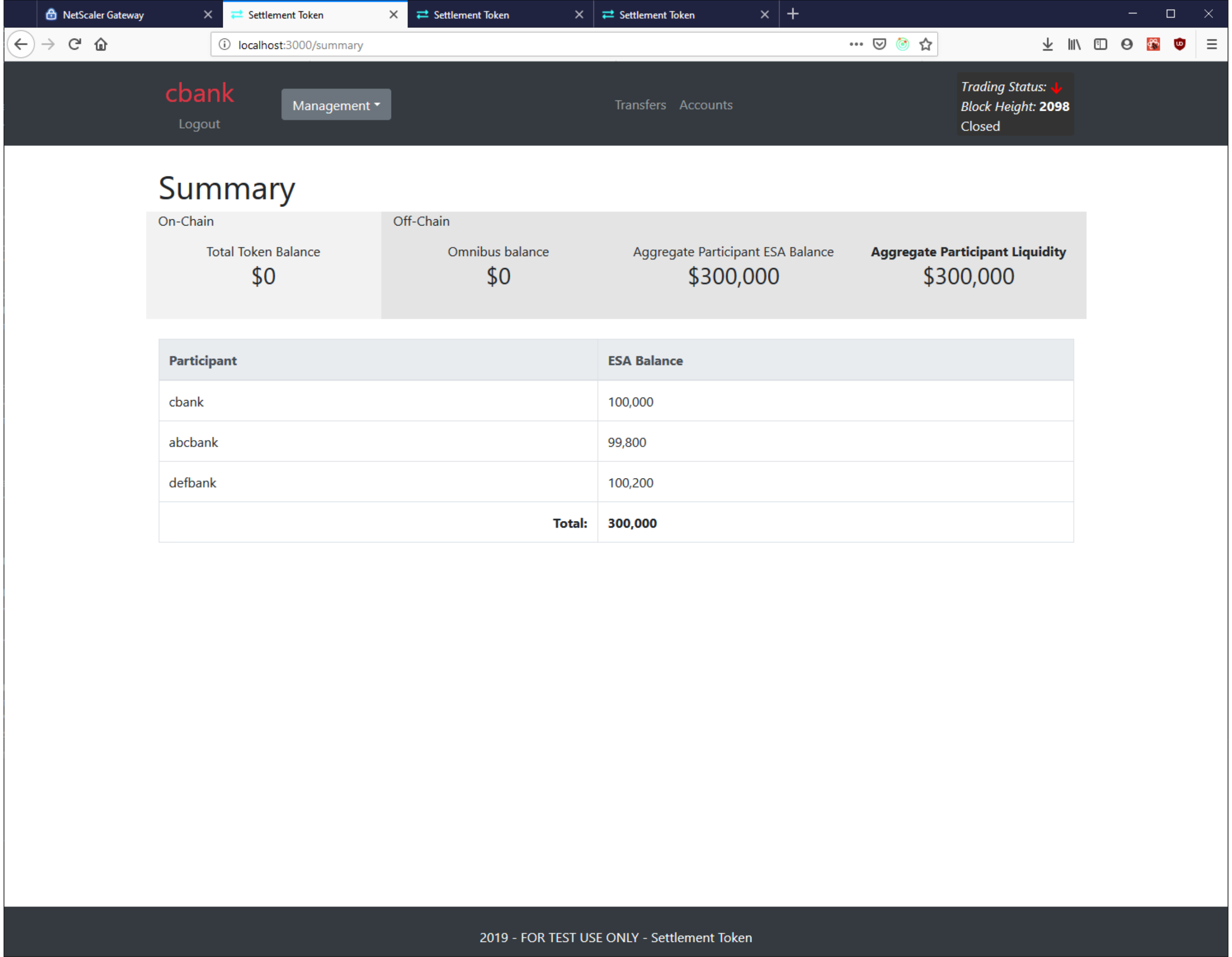
Trading Status: ↓
Block Height: **2092**
Closed

Sweep

Pending Sweep

Date	Tokens Redeemed	Status	Estimated Time	Action
7/2/2019, 3:27:00 PM	500	7/7	Complete	Balance

2019 - FOR TEST USE ONLY - Settlement Token



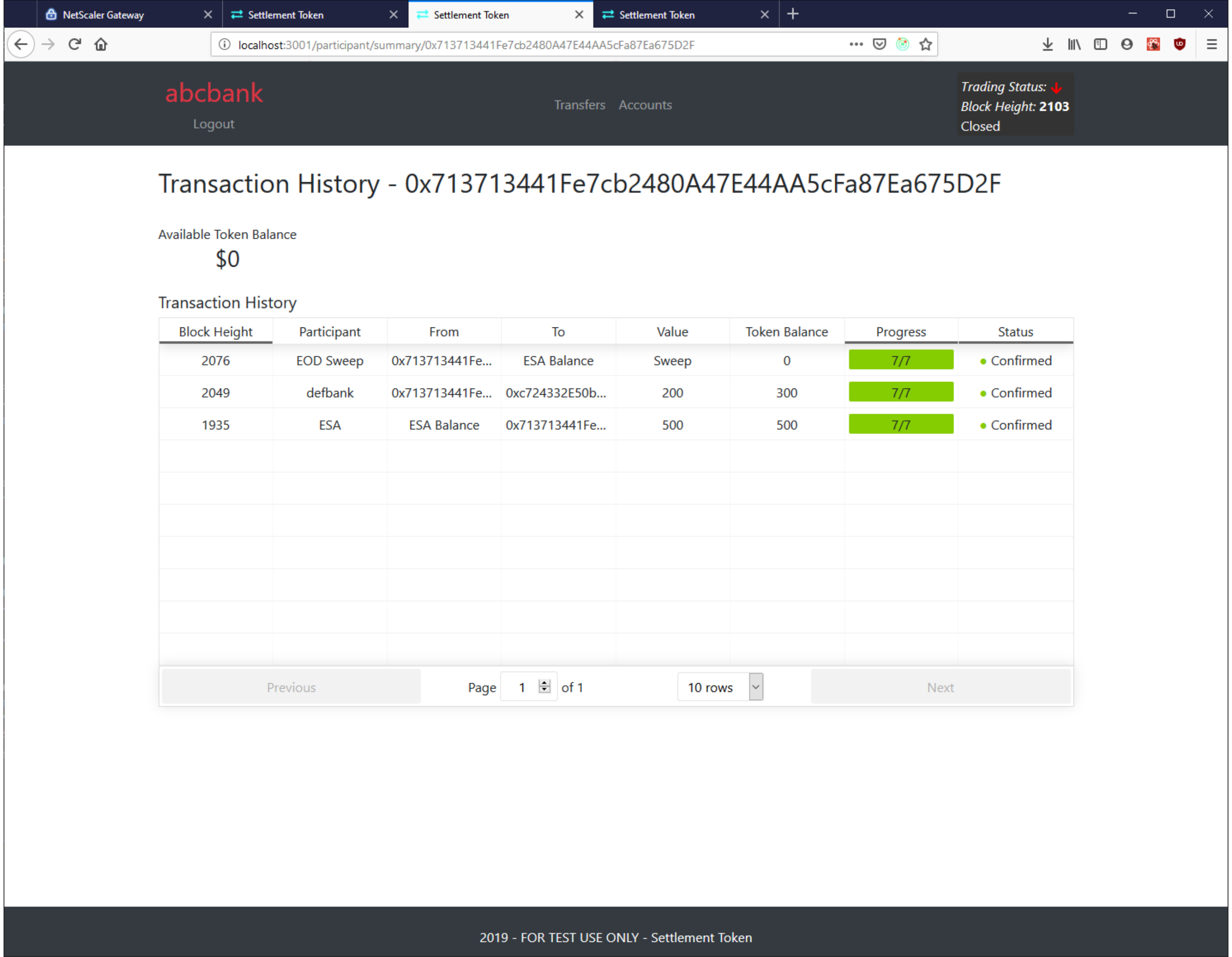
Trading Status: ↓
Block Height: **2098**
Closed

Summary

On-Chain	Off-Chain		
Total Token Balance	Omnibus balance	Aggregate Participant ESA Balance	**Aggregate Participant Liquidity**
$0	$0	$300,000	$300,000

Participant	ESA Balance
cbank	100,000
abcbank	99,800
defbank	100,200
Total:	**300,000**

2019 - FOR TEST USE ONLY - Settlement Token



Trading Status: ↓
Block Height: **2103**
Closed

Transaction History - 0x713713441Fe7cb2480A47E44AA5cFa87Ea675D2F

Available Token Balance
$0

Transaction History

Block Height	Participant	From	To	Value	Token Balance	Progress	Status
2076	EOD Sweep	0x713713441Fe...	ESA Balance	Sweep	0	7/7	● Confirmed
2049	defbank	0x713713441Fe...	0xc724332E50b...	200	300	7/7	● Confirmed
1935	ESA	ESA Balance	0x713713441Fe...	500	500	7/7	● Confirmed

2019 - FOR TEST USE ONLY - Settlement Token

Key learnings

1. Privacy
2. Security and resilience
3. Finality
4. Throughput
5. Efficiency
6. Precision

Recap

- Working solution for interbank payments on a blockchain
  - Proof of concept, technical and policy papers
  - Improved operational resilience compared to RITS
  - Resolved the lack of concept of time
- Key learnings highlight the limitations of the PoC
- Some limitations can only be addressed by pivoting to another platform

Next steps

- Move to an enterprise-grade platform
- Possible extensions include:
  - Replicating PoC in an enterprise-grade platform
  - Increasing functionality of PoC e.g. 24/7 and interest payments
  - Non-bank wholesale payments
  - Cross-border bank wholesale payments

SETTLEMENT TOKEN EXPERIMENT – PHASE 1[1]

The first phase of the Settlement Token experiment aimed to develop PY's practical understanding of distributed ledger technology (DLT) to help determine whether there is a case for the Bank to issue a wholesale settlement token using DLT. The experiment simulated a settlement system in which the central bank and a number of commercial banks were represented as nodes on a distributed ledger. This note provides an overview of the experiment, summarises key findings, and outlines possible next steps.

Background

The Settlement Token experiment was designed to expand PY's knowledge and assess the feasibility of a DLT-based wholesale settlement token by producing a proof of concept (POC). The POC simulates a settlement system, in which the central bank and a number of commercial banks are represented as nodes on a distributed ledger. Participants request tokens from the central bank in exchange for exchange settlement account (ESA) balances to use to settle their obligations on the distributed ledger throughout the trading day (Table 1).[2] The system was limited to the standard RITS hours to explore the potential of a DLT-based system as an alternative to RITS. This feature of the POC is different from other central bank projects, which have typically run on a 24/7 basis. Transactions are recorded on the ledger once the smart contract and other participants have validated that the paying entity has sufficient tokens to meet their obligations.[3] The POC was designed on the assumption that all participants are honest.[4]

Table 1: Settlement Token Timeline

Approvals (07:00-07:30)	**Start of day (07:30)**	**Intraday (07:30-22:00)**	**End of day (22:00)**
Trading closed	***Trading open***	***Trading open***	***Trading closed***
Commercial banks may request access to the network, and/or tokens in exchange for ESA balances Central bank approves or denies these requests	Central bank mints and distributes tokens as per approved commercial bank requests	Commercial banks use tokens to settle obligations Commercial banks may request the redemption of tokens for ESA balances	Central bank sweeps back and destroys tokens, then reconciles token balances with ESAs

Technical set up

The POC was built on Ethereum and hosted by a cloud service, with no connection to Bank servers. Ethereum was chosen as the most widely used open source platform for smart contracts with a large developer and support base. The POC is private and permissioned; only approved entities may access and transact on the system. The smart contract is deployed to participant nodes to improve resilience, allowing participants the ability to transact between themselves even if the central bank node goes offline.

Access

The central bank owns the smart contract containing the framework and rules providing the ability for participants to request tokens and transact on the distributed ledger. However, it cannot access or control participant nodes; participants handle their own public/private key pairs (the equivalent of a username and password). Commercial banks must request approval from the central bank to become a participant node to access the system. This process is completed 'on-chain' – on the distributed ledger – to ensure that only approved participants on the smart contract can request, send, receive, and redeem tokens on the network. Additionally, the on-chain identification of participants enables the central bank to determine how much

[1] The experiment was sponsored by PY and brought together the following staff from PY and IT to collaborate in the Innovation Lab: Cameron Dark, Anna Douderina, David Emery, June Ma, Clare Noone, Susan Slocum, Jaan Smith, Ed Tellez, and Chris Thompson. We are also grateful to Michael Shen for providing advice on the operational design of the POC throughout the experiment. For more information on the Innovation Lab, please contact Susan Slocum

[2] ESAs are the means by which providers of payments services settle obligations that have accrued in the clearing process.

[3] Smart contracts are self-executable computer programs used to manage the performance of contracts.

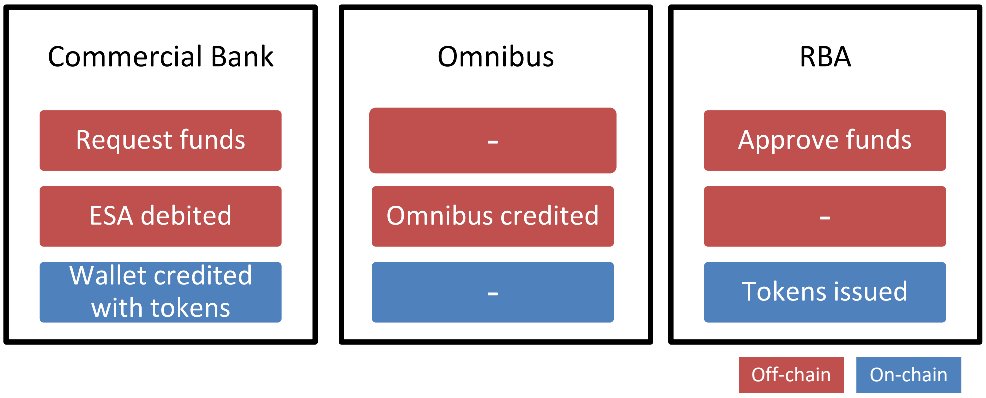
[4] This is likely to hold for the POC as it is permissioned – access is restricted to participants approved by the central bank. The assumption is important as the presence of dishonest miners could undermine the security of the system through double spending attacks or the reversal of legitimate transactions, especially if dishonest miners control the majority of nodes.

each ESA is to be credited at the end of day sweep. Participants may have multiple addresses, which enables the separation of transactions for different parts of a business.

Start of day

Prior to the trading day, approved participants may request tokens from the central bank to use at the start of day. Only one token request may be made at a time per address, though participants may cancel unapproved requests and submit a new request (e.g. if they wish to request a different number of tokens, though participants may request or redeem tokens at any time while trading is open). The central bank approves requests if the participant has a sufficient ESA balance. Tokens are credited to the participant's Ethereum address at the start of day, and the corresponding value debited from their ESA and placed into an omnibus account (Figure 1). The omnibus account holds all ESA balances that are in circulation as tokens on the smart contract, so that the central bank is not required to reconcile accounts after each transaction.

Figure 1: Token request and approval process



Intraday

Participants may request, transact, and redeem tokens throughout the day. For the purposes of the experiment, participants identify each other by providing their Ethereum address off-chain through traditional channels (for example, by email or telephone). The validity of the address on the system is verified by the smart contract, and the participant's identity is populated by the user interface. Transactions are initiated on a 'push' basis, as tokens cannot be transferred without the public and private keys of the payer.

The central bank can observe transactions made between participants but does not monitor them; it has no role in approving or rejecting these transactions. The central bank can, however, freeze funds and accounts if unusual activity has been detected. The approval of transactions is facilitated by participant nodes who compete to validate blocks of transactions.[5] The decentralisation of the validation process improves the resilience of the system and prevents double spending, since any attempts are visible to all nodes on the distributed ledger. The Ethereum protocol automatically rejects transactions if there are insufficient funds.

Users may request the redemption of tokens into ESA balances during the day. Tokens amounting to the balance of the request are frozen to ensure that they are not traded before the central bank approves the request. The central bank can calculate the number of tokens each participant has at any point in time off the distributed ledger as participants are identified on-chain. As with token requests, unapproved redemption requests may be cancelled or overridden. This permits the participant to regain liquidity from frozen funds if the central bank is offline, during which their ESA cannot be credited.

End of day

A banner appears in the user interface at 21:30 to warn participants that they are required to make all payments before 22:00. At 22:00, the ability to transact is disabled to provide sufficient time for pending

[5] Ethereum uses a 'proof of work' consensus mechanism, which is a competition between 'miner' nodes on the network to solve a cryptographic puzzle. The miner who solves the puzzle adds the associated block of transactions to the distributed ledger. This process requires time, computational, and energy resources. While the solution to the puzzle has no intrinsic value, its purpose (in public and unpermissioned systems for which it was initially developed) is for nodes to 'work' for voting rights.

transactions to be processed before the central bank conducts a sweep of tokens at the end of day.[6] Funds are frozen to prevent double spending, and all attempted transactions are automatically rejected by the smart contract. The central bank has the ability to modify this time as required to extend trading. Once all pending transactions have been processed, the central bank manually initiates the sweep. Tokens are swept into the central bank's account from participant wallets and destroyed, and funds held in the omnibus account are reconciled with participant ESAs. This is the only time of the day at which the central bank calculates the token balances of each participant using the distributed ledger.

Key learnings

The experiment resulted in a working POC of a DLT-based wholesale settlement system. While the POC has not overturned previously reported findings from other central banks, PY has furthered its understanding of the technology through practical interaction. The key learnings are discussed below.

Privacy

While Ethereum provides a good foundation to develop a practical understanding of DLT, it does not afford an adequate level of privacy as transactions are visible by all nodes. In Ethereum, participant addresses are represented as alphanumeric strings, which have no relationship to the participant's identity. Where there are a large number of participants and addresses, it is difficult, though not impossible, to deduce identities by tracing through transactions on the distributed ledger. However, for a wholesale settlement system limited to approved participants, it would be much simpler to deduce identities through interactions on the system, given that each participant will know the addresses of the entities with whom it has interacted.

From the perspective of a central bank, complete privacy is not desirable for both operational and security reasons. Within the POC, it is necessary for the central bank to have knowledge of the identities of participants in order to provide them with access to the system, approve their token requests, and to reconcile their token balances with their ESA at the end of day. While the central bank would not use this knowledge to track all transactions, it would be able to intervene if any suspicious or malicious activity were identified.

Ideally, the central bank would have complete knowledge of participant identities and the ability to gain visibility over transactions as required, while participants would have no visibility over transactions other than their own. This is not currently possible using Ethereum, and is a key consideration in determining the choice of platform for future phases of the experiment.

Security and resilience

A focus of the experiment was to decentralise processes as much as possible to explore the potential and limitations of DLT, with security being a less important factor for the purposes of the POC. The decentralisation of the POC improves resilience relative to RITS by allowing participants to continue trading even if the central bank node goes offline. However, the POC demonstrated a trade-off between security (as implemented by the requirement of central bank approval for access and token requests) and resilience. The central bank's unique role in enforcing the security of the POC means that participants lose some functionality if the central bank goes offline, as no requests to access the system or for tokens will be approved. This would be a problem where an entity does not have sufficient liquidity to settle their obligations on the platform. This trade-off may be partially overcome by having multiple central bank nodes, similar to the Bank's current business continuity plan for RITS.

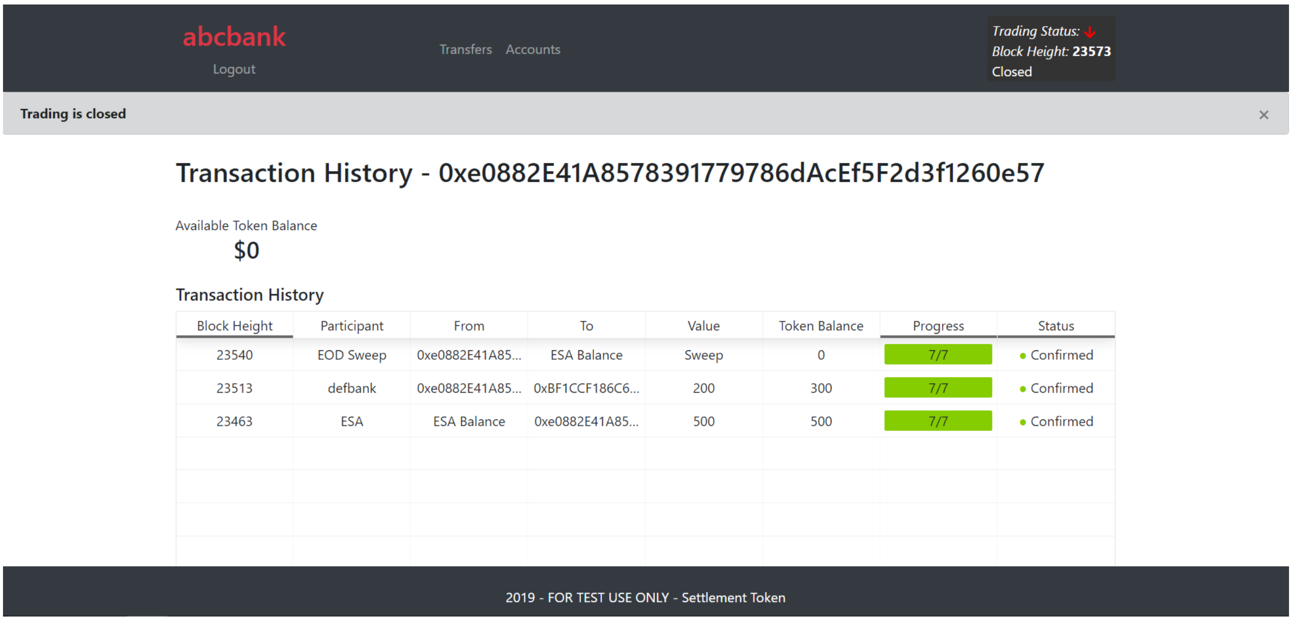
Finality

Theoretically, transactions on proof-of-work-based distributed ledgers such as Ethereum are never final as there is always a non-zero probability that they can be reversed. Delayed transaction finality arises from the potential for multiple blocks to be confirmed simultaneously, or from attacks on the system. Both scenarios result in the reversal of transactions (though the latter would be unlikely to occur given access is restricted

[6] The end of day process technically commences at the block height that the system is estimated to reach at 22:00. Therefore, the process may not commence exactly at 22:00. This estimation takes place when the central bank sets the time it wishes to disable transactions, and can be updated throughout the day. Block height is used as Ethereum has no trusted centralised concept of time, with scheduling based on the number of blocks. While transactions are timestamped, the decentralised nature of Ethereum means that this time may differ between nodes.

to approved participants in the POC). However, the probability of finality increases exponentially with the addition of each subsequent block, provided there are more honest participants than malicious participants. For this reason, the rule of thumb in Ethereum is to wait six blocks after a transaction has been confirmed before considering it to have reached finality. This is equivalent to approximately a minute, but can vary according to network activity. Given the importance and scale of a wholesale settlement system, a longer confirmation period of seven blocks was adopted for the purposes of the POC (Figure 2). In the POC, participants are unable to use funds until seven confirmations have been reached to ensure that those funds are actually available to them. This is slower than RITS, in which finality is reached in real time.

Figure 2: Transaction History



Trading Status: ↓
Block Height: **23573**
Closed

Trading is closed ×

Transaction History - 0xe0882E41A8578391779786dAcEf5F2d3f1260e57

Available Token Balance
$0

Transaction History

Block Height	Participant	From	To	Value	Token Balance	Progress	Status
23540	EOD Sweep	0xe0882E41A85...	ESA Balance	Sweep	0	7/7	● Confirmed
23513	defbank	0xe0882E41A85...	0xBF1CCF186C6...	200	300	7/7	● Confirmed
23463	ESA	ESA Balance	0xe0882E41A85...	500	500	7/7	● Confirmed

2019 - FOR TEST USE ONLY - Settlement Token

Throughput

The throughput – the number of transactions per second – of Ethereum is slow at 12 transactions per second compared with existing payment systems. While it is possible to increase throughput in Ethereum to speed up transaction finality, this increases the probability of forks. Forks occur when multiple blocks are confirmed simultaneously, temporarily splitting the ledger at that point. While the network eventually resolves forks as subsequent blocks are confirmed, the blocks that are not part of the main chain are 'orphaned', and must be reconfirmed. The avoidance of forks is particularly important in the POC due to on/off chain interaction between ESAs and Settlement Token accounts. For example, an on-chain request for tokens could result in an ESA being debited, but no tokens being credited to the Settlement Token account if the block containing the request was on a fork. Accordingly, delayed transaction finality is essential to minimise such occurrences.

Efficiency

Ethereum uses proof of work as its consensus mechanism, which is a competition between nodes to verify and process transactions. This requires substantial time, computational, and energy resources that are effectively wasted. This is highlighted by the discrete trading sessions in the experiment; nodes must continue mining empty blocks overnight due to the dynamic adjustment of difficulty in Ethereum to maintain the throughput rate. If no blocks are mined overnight, then the difficulty of the proof of work would fall, leading blocks to be mined at a faster rate at the start of the following day, increasing the probability of forks.

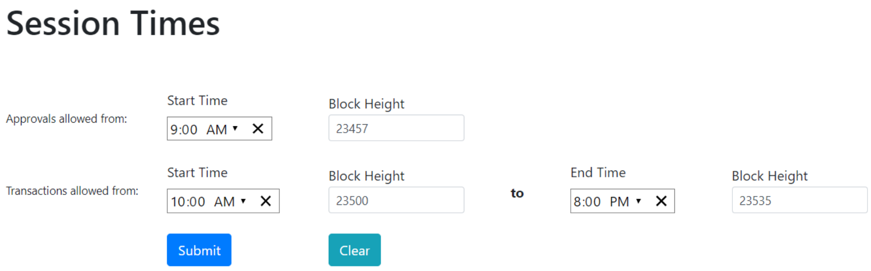
In a trusted and private environment, nodes should be able to coordinate to validate transactions in a round robin manner to improve the efficiency of the network. This is fundamentally contrary to proof of work, and can only be resolved through the use of an alternative platform that uses a different consensus mechanism.

Precision

The decentralisation of the DLT-based networks mean that there is no centralised concept of time agreed upon by all nodes. Blocks of transactions are time stamped on the ledger according to the time of the participant who mined the block, which may differ from the system time of other nodes on the network. As a result, DLT-based networks rely on block height to determine the order of events, contrary to the design of the POC, which is intended operate on the basis of time in line with RITS.

To overcome this limitation, the POC uses the average rate at which blocks are mined as determined by the Ethereum network (12 seconds) to estimate the block height that will occur at the certain times, and uses these block heights to enable or disable smart contract functionality as desired. However, this approach lacks precision as the mining rate is probabilistic and can also change according to changes in the aggregate computational power of the network. This means that session times are unlikely to start at the exact time desired. For example, transactions will be allowed from the block height of 23500, regardless of whether it is reached before or after 10:00 (Figure 3). Since the mining rate will change over time, the closer a session time is set to its desired time, the more accurate it will be.

Figure 3: Estimation of Block Height from Session Times



Session Times

Approvals allowed from: Start Time 9:00 AM; Block Height 23457

Transactions allowed from: Start Time 10:00 AM; Block Height 23500 to End Time 8:00 PM; Block Height 23535

Next steps

The next phase of the experiment will seek to address the limitations identified in the first phase. Some of these limitations will be addressed by moving to an enterprise-grade DLT platform such as JP Morgan's *Quorum*, R3's *Corda*, or IBM's *Hyperledger*. In addition, the next phase will extend the POC to allow tokens to be distributed by commercial banks to non-bank wholesale market participants for the settlement of digital assets on a separate DLT platform.

June Ma
Senior Analyst
Payments System Efficiency
Payments Policy Department
5 December 2019