

Azure SQL Database Ledger

Gianluca Hotz

@glhotz

Data Platform MVP - Presidente UGISS.ORG



Chi sono?

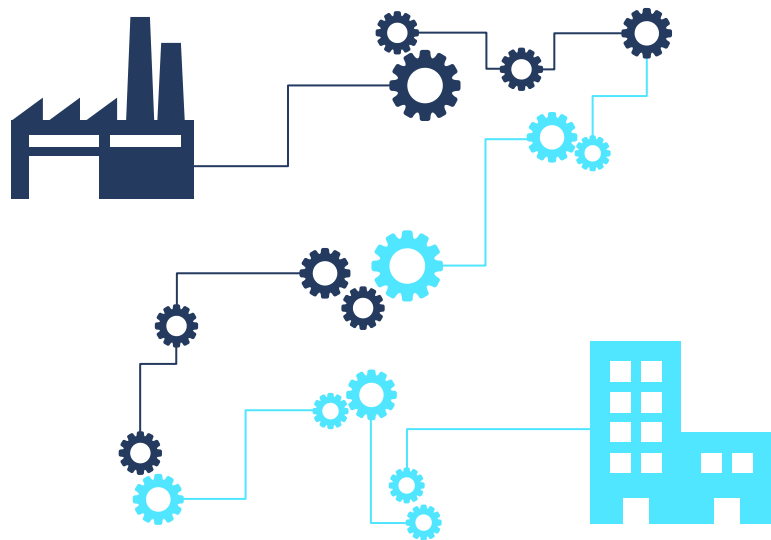


- Gianluca Hotz | @glhotz | ghotz@ugiss.org
- Consulente indipendente
 - 25 anni su SQL Server (dalla 4.21 nel 1996)
 - Modellazione e sviluppo database, dimensionamento e amministrazione database server, aggiornamenti e migrazioni, performance tuning
- Community
 - 23 anni Microsoft [MVP](#) SQL Server/Data Platform (dal 1998)
 - VMware Experts SQL Server
 - Fondatore e presidente [UGISS](#) (ex «PASS Chapter»)
 - (Co-organizzatore DAMAG Meetup Community)



Tecnologie «Ledger» e «Digital Trust»

Le aziende si stanno spostando da intermediari e audit manuali che sono **lenti** e **costosi**...



...a tecnologie «Ledger» che **riducono i costi**, fanno **risparmiare tempo** e **riducono i rischi**



Previsioni crescita mercato «blockchain»

1,213 views | May 13, 2020, 10:03am EDT

Will Enterprise Blockchain Survive? Report Puts Blockchain Market At **\$21 Billion By 2025**

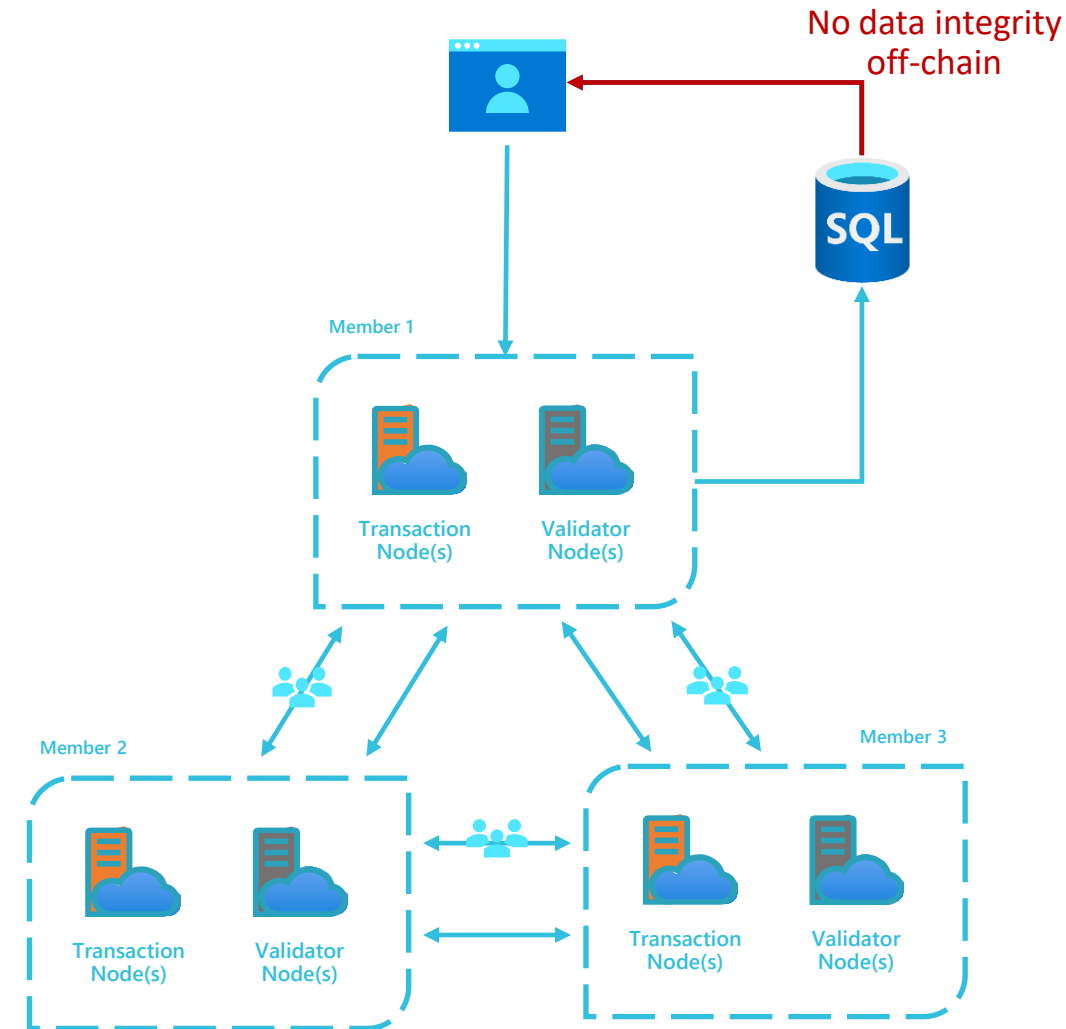
<https://www.forbes.com/sites/robertanzalone/2020/05/13/will-enterprise-blockchain-survive-a-new-report-says-that-the-blockchain-technology-market-will-reach-21-billion-by-2025/#7a5f793954b8>

Ninety percent of permissioned blockchain projects are misaligned to blockchain technology, because they remain centralized database projects at the core. These projects can be implemented more quickly, more cost-effectively, and with less risk and higher quality by avoiding blockchain altogether.

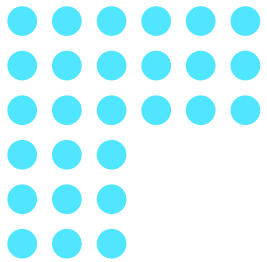
Gartner Predicts 2019: Blockchain Technologies

«Blockchain» esagerate in scenari centralizzati

- Decentramento richiede a tutte le parti di ospitare nodi per partecipare al consenso
- Regole di «governance» devono essere stabilite dal consorzio e distribuite/gestite
- Latenza associata a consenso può influire su velocità effettiva transazioni (<1000 TPS per «Ethereum»)
- Archiviazione «off-chain» per interrogazioni è tipica, ma integrità si perde nel processo
- Sistemi personalizzati con tool immaturi rendono **sviluppo e gestione impegnativi**



Azure SQL Database Ledger



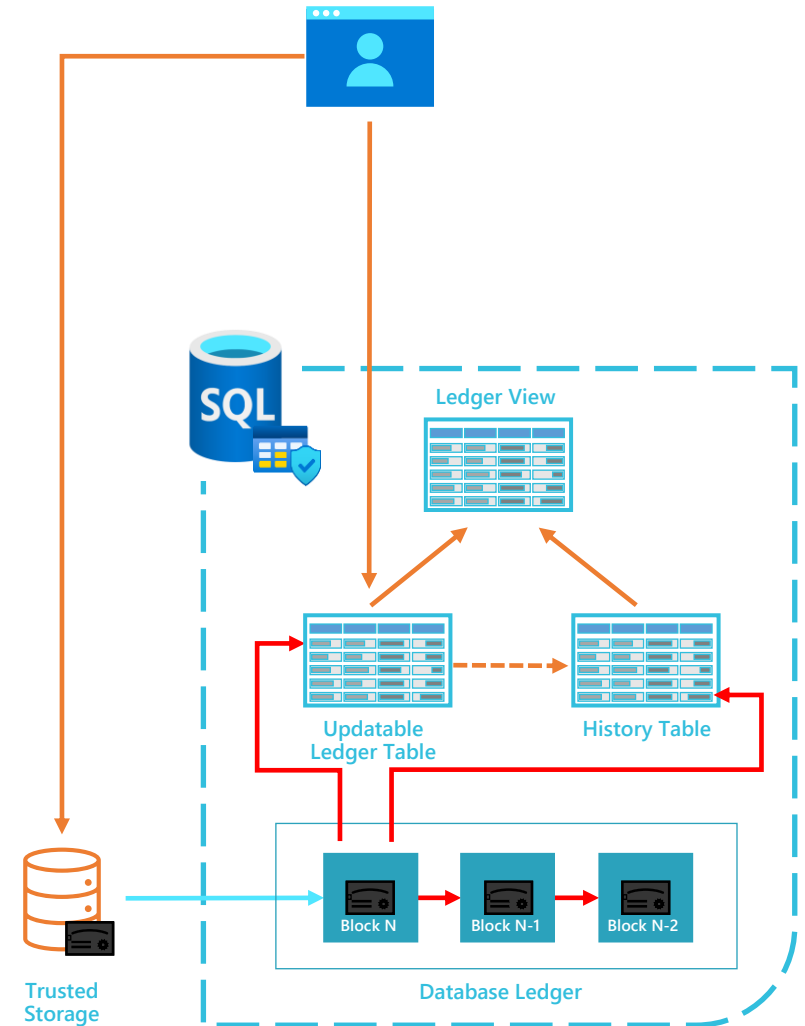
Rende dati in SQL a prova di manomissione tramite crittografia

Fornisce traccia cronologica delle modifiche, verificata tramite prove crittografiche

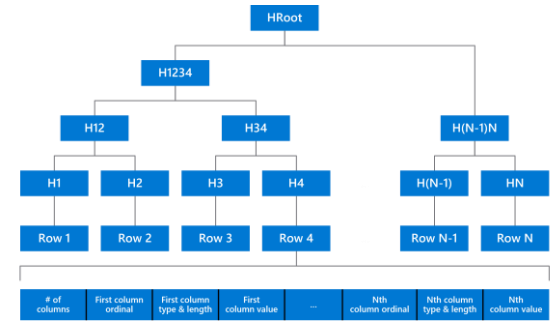
Lo stesso SQL Server già usato in Azure e «on-premises»

Tabelle «Ledger»

- **«Updatable»** permettono «insert/update/delete»
- Cronologia aggiornamento mantenuta tabella storica e nella «Ledger View» di facile consultazione
- Integrità tabelle «aggiornabile» e «storico» mantenuta tramite collegamenti crittografici nel «Database Ledger»
- Ricevute digitali caricate periodicamente in storage attendibile configurato dal cliente
- Cliente può utilizzare ricevute digitali per verificare integrità dei dati
- **«Append-Only»** permesso solo «insert»
 - rimuovono necessità tabella «storico»



«Database Ledger»



- Cattura incrementalmente stato database
 - A livello logico: «blockchain» e strutture dati «Merkle Tree»
 - Cattura anche metadati transazione (es. timestamp, utente)
- Blocchi e informazioni transazioni in tabelle di sistema
 - sys.database_ledger_transactions
 - sys.database_ledger_blocks
- Blocchi chiusi
 - ogni 30 secondi
 - oppure esecuzione manuale sys.sp_generate_database_ledger_digest

«Database Digest»

- Hash ultimo blocco «Ledger»
 - Rappresenta stato di tutte le tabelle «Ledger»
- Devono essere mantenuti in uno storage affidabile e immutabile
 - Altrimenti si potrebbero manomettere le informazioni (in teoria)
- Possibilità di generarli manualmente o in automatico
- Generati in automatico possono essere anche salvati in automatico
 - «Immutable Blob Storage»
 - «Azure Confidential Ledger» (ACL)

Storage attendibile

«Immutable Blob Storage»

- Storage «Write Once, Read Many» basato su **policy**
- BLOB possono essere impostati in sola lettura per intervallo specificato
- Dati bloccati solo funzionalmente in base a policy
- Supporto per «audit logging» ma creatore log deve essere considerato attendibile
- Microsoft è la «Trusted Computing Base»

«Azure Confidential Ledger» (ACL)

- Storage «Write Once, Read Many» in **perpetuo**
- BLOB scritti nel «Ledger» non possono essere modificati
- Utilizza «Confidential Enclaves» a prova di manomissione
- Crea ricevute transazioni e file «Ledger» serializzati contenenti informazioni che possono essere verificate dai clienti
- Microsoft è fuori dalla «TCB», codice sorgente è open source (Confidential Consortium Framework)

Verifica del «Ledger»

- Manomissione possibile a meno di modifiche impedito/tracciate
 - Es. modifica diretta file dati, DBCC WRITEPAGE ecc.
- Verifica ricalcola tutti gli hash e li confronta con i «digest»
 - Operazione richiede uso intensivo di risorse
- Verificare
 - quando necessario (es. sospetto manomissione, audit)
 - su base ricorrente (es. giornalmente, ogni ora)
- Verifica tramite procedura di sistema dipende da modalità salvataggio
 - automatico: passando indirizzo storage
 - manuale: passando documento JSON con «Digest»

«Ledger auditing»

- Nuovi eventi SQL Audit
 - ENABLE LEDGER
 - Creazione tabelle (o conversione, non ancora supportata)
 - ALTER LEDGER
 - Eliminazione/cambio nome tabelle (non ancora supportati)
 - GENERATE LEDGER DIGEST
 - VERIFY LEDGER
 - LEDGER_OPERATION_GROUP

Demo

Abilitazione Database Ledger

Selezione opzione «deployment»


[Home](#) > [All resources](#) > [Create a resource](#) > [Azure SQL](#) >

Select SQL deployment option ...

Microsoft

[Feedback](#)

How do you plan to use the service?


**SQL databases**

Best for modern cloud applications. Hyperscale and serverless options are available.

Resource type

Single database

[Create](#) [Hide details](#)


**SQL managed instances**

Best for most migrations to the cloud. Lift-and-shift ready.

Resource type

Single instance


[Create](#) [Show details](#)

**SQL virtual machines**

Best for migrations and applications requiring OS-level access. Lift-and-shift ready.

Image


[Create](#) [Show details](#)

**Single database**

Single databases are a great fit for modern, cloud-born applications that need a fully managed database with predictable performance.

Featured capabilities:


- ✓ Hyperscale storage (up to 100TB)
- ✓ Serverless compute
- ✓ Easy management

**Elastic pool**

Elastic pools provide a cost-effective solution for managing the performance of multiple databases with variable usage patterns.

Featured capabilities:

- ✓ Resource sharing for cost optimization
- ✓ Simplified performance management

**Database server**

Database servers are used to manage groups of single databases and elastic pools.

Featured capabilities:

- ✓ Access management
- ✓ Backup management
- ✓ Business continuity management




Creazione Database

[Home](#) > [All resources](#) > [Create a resource](#) > [Azure SQL](#) > [Select SQL deployment option](#) >

Create SQL Database

Microsoft

 Changing Basic options may reset selections you have made. Review all options prior to creating the resource.

[Basics](#) [Networking](#) [Security](#) [Additional settings](#) [Tags](#) [Review + create](#)

Create a SQL database with your preferred configurations. Complete the Basics tab then go to Review + Create to provision with smart defaults, or visit each tab to customize. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *  Pay-As-You-Go

Resource group *  (New) Demos

[Create new](#)

Database details

Enter required settings for this database, including picking a logical server and configuring the compute and storage resources


Database name * lgdemo

Server *  (new) ledgerdemo (West Central US)

[Create new](#)

Want to use SQL elastic pool? * 

☐ Yes ☒ No

Compute + storage * 


General Purpose

Serverless, Gen5, 1 vCore, 3 GB storage

[Configure database](#)


Backup storage redundancy


Choose how your PITR and LTR backups are replicated. Geo restore or ability to recover from regional outage is only available when geo-redundant storage is selected.

Backup storage redundancy 

☐ Locally-redundant backup storage - Preview

☒ Geo-redundant backup storage

 Selected value for backup storage redundancy is Geo-redundant backup storage. Note that database backups will be geo-replicated to the paired region. [Learn more](#)

 Your use of either of the Preview backup storage redundancy options (ZRS and LRS) is governed by the agreement under which you obtained Microsoft Azure Services. By selecting a Preview redundancy option, you confirm that you agree to the preview terms in such agreement. Microsoft Azure Legal Information: [Learn more](#)

[Review + create](#)

[Next : Networking >](#)



Configurazione «Ledger»

[Home](#) >

Create SQL Database ...

Microsoft

Basics Networking **Security** Additional settings Tags Review + create

Azure Defender for SQL

Protect your data using Azure Defender for SQL, a unified security package including vulnerability assessment and advanced threat protection for your server. [Learn more](#)

Get started with a 30 day free trial period, and then 12.6495 EUR/server/month.

Enable Azure Defender for SQL * ⓘ ☐ Start free trial
☒ Not now

Ledger (preview)

Ledger cryptographically verifies the integrity of your data and detects any tampering that might have occurred. [Learn more](#)

Ledger (preview) **Not configured**
[Configure ledger](#)

[Home](#) > [Create SQL Database](#) >

Configure ledger (preview) ...

Create SQL Database

ⓘ Azure SQL Database Ledger and Azure Confidential Ledger are each currently in preview. By using this preview feature, you confirm that you agree that your use of this feature is subject to the preview terms in the agreement under which you obtained Microsoft Azure Services. [Learn more](#)

Ledger (preview)

Enabling ledger functionality **will make all tables in your database ledger tables that can be updated**. This option **cannot be changed after you create your database**. If you do not select this option now, you can create ledger tables that can be updated or only appended to when creating new tables using T-SQL. After enabling ledger functionality for a table, you cannot disable this option. [Learn more](#)

Enable for all future tables in this database ☐

Digest storage

If you want ledger to **generate digests automatically and store them** for your verification later, you need to configure an Azure Storage account or Azure Confidential Ledger. **Alternatively, you can manually generate digests and store them in your own secure location**. [Learn more](#)

Enable automatic digest storage ⓘ ☐



«Digest Storage»

[Home](#) > [Create SQL Database](#) >

Configure ledger (preview) ...

Create SQL Database

i Azure SQL Database Ledger and Azure Confidential Ledger are each currently in preview. By using this preview feature, you confirm that you agree that your use of this feature is subject to the preview terms in the agreement under which you obtained Microsoft Azure Services. [Learn more](#)

Ledger (preview)

Enabling ledger functionality will make all tables in your database ledger tables that can be updated. This option cannot be changed after you create your database. If you do not select this option now, you can create ledger tables that can be updated or only appended to when creating new tables using T-SQL. After enabling ledger functionality for a table, you cannot disable this option. [Learn more](#)

Enable for all future tables in this database ☐

Digest storage

If you want ledger to generate digests automatically and store them for your verification later, you need to configure an Azure Storage account or Azure Confidential Ledger. Alternatively, you can manually generate digests and store them in your own secure location. [Learn more](#)

Enable automatic digest storage ⓘ ☒

Storage type
☒ Azure Storage
☐ Azure Confidential Ledger (Preview)

Storage account *
(new) ledgerdemostorage ▼
[Create new](#)

Storage container ⓘ
(new) sqldbledgerdigests

⚠ To prevent tampering of your digest files, configure and lock a retention policy for your container. [Learn more](#)

[Home](#) > [Create SQL Database](#) >

Configure ledger (preview) ...

Create SQL Database

i Azure SQL Database Ledger and Azure Confidential Ledger are each currently in preview. By using this preview feature, you confirm that you agree that your use of this feature is subject to the preview terms in the agreement under which you obtained Microsoft Azure Services. [Learn more](#)

Ledger (preview)

Enabling ledger functionality will make all tables in your database ledger tables that can be updated. This option cannot be changed after you create your database. If you do not select this option now, you can create ledger tables that can be updated or only appended to when creating new tables using T-SQL. After enabling ledger functionality for a table, you cannot disable this option. [Learn more](#)

Enable for all future tables in this database ☐

Digest storage

If you want ledger to generate digests automatically and store them for your verification later, you need to configure an Azure Storage account or Azure Confidential Ledger. Alternatively, you can manually generate digests and store them in your own secure location. [Learn more](#)

Enable automatic digest storage ⓘ ☒

Storage type
☐ Azure Storage
☒ Azure Confidential Ledger (Preview)

Confidential ledger * ⓘ
Create new ▼

Pricing tier
Standard Tier
Free during preview



Demo

Ledger Tables

Tabella Aggiornabile

```
CREATE SCHEMA [Account];
GO
CREATE TABLE [Account].[Balance]
(
    [CustomerID]    int                NOT NULL PRIMARY KEY CLUSTERED
,
    [LastName]      varchar(50)        NOT NULL
,
    [FirstName]     varchar(50)        NOT NULL
,
    [Balance]       decimal(10,2)      NOT NULL
)
WITH (
    SYSTEM_VERSIONING = ON --(HISTORY_TABLE = [Account].[BalanceHistory])
,
    LEDGER = ON --(LEDGER_VIEW = [Account].[BalanceLedgerView])
);
GO
```



Transazioni di inserimento

-- Prima transazione

INSERT INTO [Account].[Balance]

VALUES

(1, 'Jones', 'Nick', 50);

GO

-- Seconda transazione

INSERT INTO [Account].[Balance]

VALUES

(2, 'Smith', 'John', 500)

, (3, 'Smith', 'Joe', 30)

, (4, 'Michaels', 'Mary', 200);

GO



Selezione da tabella

-- Di default le colonne con le informazioni relative alle
-- transazioni non vengono tornate (trasparente applicazioni)

SELECT *

FROM [Account].[Balance];

GO

Results		Messages		
	CustomerID	LastName	FirstName	Balance
1	1	Jones	Nick	50.00
2	2	Smith	John	500.00
3	3	Smith	Joe	30.00
4	4	Michaels	Mary	200.00

Selezione da tabella campi aggiuntivi

-- Devono essere selezionate esplicitamente

```
SELECT *  
    , [ledger_start_transaction_id]  
    , [ledger_end_transaction_id]  
    , [ledger_start_sequence_number]  
    , [ledger_end_sequence_number]  
FROM [Account].[Balance];  
GO
```

Results		Messages							
	CustomerID	LastName	FirstName	Balance	ledger_start_transaction_id	ledger_end_transaction_id	ledger_start_sequence_number	ledger_end_sequence_number	
1	1	Jones	Nick	50.00	1420	NULL	0	NULL	
2	2	Smith	John	500.00	1423	NULL	0	NULL	
3	3	Smith	Joe	30.00	1423	NULL	1	NULL	
4	4	Michaels	Mary	200.00	1423	NULL	2	NULL	

Aggiornamento

```
UPDATE [Account].[Balance]  
SET [Balance] = 100  
WHERE [CustomerID] = 1;  
GO
```

Interrogazione dopo aggiornamento

```
-- Interroghiamo la tabella aggiornabile, quella di storico e la vista
SELECT *
,[ledger_start_transaction_id]
,[ledger_end_transaction_id]
,[ledger_start_sequence_number]
,[ledger_end_sequence_number]
FROM [Account].[Balance];

SELECT * FROM [Account].[MSSQL_LedgerHistoryFor_1525580473];

SELECT * FROM [Account].[Balance_Ledger] ORDER BY [ledger_transaction_id];
GO
```



Risultato interrogazione

Results Messages								
	CustomerID	LastName	FirstName	Balance	ledger_start_transaction_id	ledger_end_transaction_id	ledger_start_sequence_number	ledger_end_sequence_number
1	1	Jones	Nick	100.00	1432	NULL	0	NULL
2	2	Smith	John	500.00	1423	NULL	0	NULL
3	3	Smith	Joe	30.00	1423	NULL	1	NULL
4	4	Michaels	Mary	200.00	1423	NULL	2	NULL

	CustomerID	LastName	FirstName	Balance	ledger_start_transaction_id	ledger_end_transaction_id	ledger_start_sequence_number	ledger_end_sequence_number
1	1	Jones	Nick	50.00	1420	1432	0	1

	CustomerID	LastName	FirstName	Balance	ledger_transaction_id	ledger_sequence_number	ledger_operation_type	ledger_operation_type_desc
1	1	Jones	Nick	50.00	1420	0	1	INSERT
2	2	Smith	John	500.00	1423	0	1	INSERT
3	3	Smith	Joe	30.00	1423	1	1	INSERT
4	4	Michaels	Mary	200.00	1423	2	1	INSERT
5	1	Jones	Nick	50.00	1432	1	2	DELETE
6	1	Jones	Nick	100.00	1432	0	1	INSERT



Tabella «Append-Only»

```
CREATE SCHEMA [AccessControl];
GO
CREATE TABLE [AccessControl].[KeyCardEvents]
(
    [EmployeeID]                int                NOT NULL PRIMARY KEY CLUSTERED
    , [AccessOperationDescription] nvarchar(MAX)    NOT NULL
    , [Timestamp]                datetime2         NOT NULL
)
WITH (
    LEDGER = ON (APPEND_ONLY = ON)
);
GO
```

Inserimento e aggiornamento

```
-- Inseriamo una prima riga
INSERT INTO [AccessControl].[KeyCardEvents]
VALUES ('43869', 'Building42', '2020-05-02T19:58:47.1234567');
GO

-- Se proviamo a fare un'aggiornamento, da errore
UPDATE [AccessControl].[KeyCardEvents]
SET [EmployeeID] = 34184
WHERE [EmployeeID] = 43869;
GO
```

Messages

```
Msg 37359, Level 16, State 1, Line 141
Updates are not allowed for the append only Ledger table 'AccessControl.KeyCardEvents'.
```

Demo

Verifica Database

Verifica Database

The screenshot displays the Microsoft Azure portal interface for an Azure SQL Database Ledger. The main heading is "Igdemo (ledgerdemo/Igdemo) | Ledger". The left-hand navigation pane shows various management options, with "Ledger" highlighted. The right-hand pane contains the "Verify database" section, which includes a "Verify database" button (indicated by an orange arrow) and a T-SQL script for verification. The script is as follows:

```
DECLARE @digest_locations NVARCHAR(MAX) = (SELECT * FROM
sys.database_ledger_digest_locations FOR JSON AUTO, INCLUDE_NULL_VALUES);
SELECT @digest_locations as digest_locations;
BEGIN TRY
EXEC sys.sp_verify_database_ledger_from_digest_storage @digest_locations;
SELECT 'Ledger verification succeeded.' AS Result;
END TRY
BEGIN CATCH
THROW;
END CATCH
```

The "Verify database" section also includes a description of the verification process and a "Verify database" button. Below this, there are sections for "Ledger (preview)" and "Digest storage", each with configuration options and a "Learn more" link.

PREVIEW

Limitazioni generali

- Opzione a livello di database non può essere disabilitata
- No conversione tabelle esistenti
- No cambio di nome o spostamento di «schema»
- No eliminazione dati tabelle di storico (tabelle aggiornabili)
- Transazione può aggiornare solo (!) 200 tabelle
- «Long-term backups» (LTR) non supportati
- «Ledger» aggiornabili ereditano limitazioni tabelle temporali

PREVIEW

Limitazioni di interoperabilità

- Tabelle «In-memory» non supportate
- No operazioni di SWITCH IN/OUT
- No indici di tipo «Full-Text»
- No indice «non-clustered rowstore» con «clustered columnstore»
- No «Change Tracking»
- No tabelle FILETABLE
- No utilizzo API UPDATETEXT e WRITETEXT

PREVIEW

Limitazioni schema

- Numero massimo di colonne (sempre 1024)
 - Tabelle aggiornabili +4 colonne
 - Tabelle solo accodamento +2 colonne
- Aggiunta solo di colonne «nullable» (senza WITH VALUES)
- No eliminazione colonne, modifica limitata:
 - NULL/NOT NULL, lunghezza tipi a lunghezza variabile, SPARSE
 - «Collation» per tipi Unicode, se non cambia «code page» per gli altri
- No tipi dato XML, FILESTREAM, SqlVariant e «user-defined»
- Colonne «computed» solo deterministiche
- No «Sparse Column Set»

Scenari per tabelle «Ledger»

- In generale: quelli che necessitano solo della «Forward Integrity»
 - Sistema attendibile al processamento della transazione, protetto contro manomissioni future
- Alcuni esempi
 - Semplificazione scenari di audit
 - Verifica crittografica manomissione dati verso terze parti (interne o esterne)
 - Processi aziendali tra più parti
 - Alternativa a «blockchain» per sistemi intrinsecamente centralizzati in ottica «trust, but verify»
 - Storage «off-chain» affidabile per interrogazioni dati «blockchain»
- «Choosing an Azure ledger technology»
 - <https://techcommunity.microsoft.com/t5/azure-sql/choosing-an-azure-ledger-technology/ba-p/2450502>



Risorse

- Announcement blog
 - <https://aka.ms/sql-ledger-blog>
- Azure SQL Database ledger Documentation
 - <https://aka.ms/sql-ledger-docs>
- Whitepaper
 - <https://aka.ms/sql-ledger-whitepaper>

Grazie!

- Il materiale sarà online nei prossimi giorni su <http://www.communitydays.it>