

BTG UNIVERSAL FOUNDRY ARCHITECTURE

Technical responsibilities, data contracts, permissions and deployment lifecycle

THE COMPLETE SYSTEM DESIGN · OCTOBER 2026

The completed BTG Universal Technology Foundry is a unified technology creation, repair, execution and economic infrastructure platform. Every component belongs to one lifecycle: preserve the original, understand what it does, develop improvements, validate behavior, operate under authorization, and record actual economic use. The platform is being engineered toward this completed architecture; the description is a specification of that destination rather than a claim that each production connection is live today.

Reader note: this document defines the completed platform and intended operations. Current implementation evidence is available separately through the Development Centre.

CHAPTER LEGEND & CONTENTS

01 Purpose and boundaries

02 Component ownership

03 Contract structure

04 Technical acceptance

05 Cross-product user journey

06 Run-time isolation

07 Operations and incident response

08 Rollout sequence

Purpose and boundaries

The BTG Universal Technology Foundry is a shared platform with a single set of trusted foundations. This architecture guide identifies how applications, operators and rights holders interact with the same core services.

It is a completed-design specification and not a claim that all hardware or software integrations currently satisfy release requirements.

Component ownership

BTG Studio owns the importer and graphical construction experience; NIKI owns proposal and review orchestration; ADAM/BTDU owns canonical execution and knowledge; FarmNodes own authorized physical job execution; ENTITY owns identities, rights and revocation; Bridge owns contribution and data permissions; Bit Trade Global owns asset/instrument disclosure and market ledger functions.

None of these services can silently create a second authoritative copy of another service’s records.

Contract structure

Every approved DataChip declares types, version, required resources, bound owner permissions, evidence hashes and failure modes. Each Circuit references exact chip versions. A Genome references exact components and an acceptance manifest. A user’s imported files are immutable external inputs rather than shareable defaults.

Schema evolution requires version compatibility tests, migration mappings and rollback. Signed evidence is never overwritten to make a newer result appear originally present.

Technical acceptance

An imported system must have a reproducible baseline. Repair outputs need independent evaluation. A physical FarmNode records OS-observed resources, verified device identity, enforced limits and result receipts. Native application release includes actual signed builds and physical target tests.

The Council must demonstrate distinct independent model evaluations and source-grounded judgments. Model roster labels alone are not sufficient for production decisions.

Cross-product user journey

The owner signs in through ENTITY, brings a source archive to Studio, reviews the inferred dependency graph, authorizes requested model and resource access, selects a repair or build target and inspects evidence. A qualified Genome then operates through a suitable host.

Bridge gives contributors granular control; Bit Trade Global identifies assets and rights and provides commercial/financial workflows only as separately authorized.

Run-time isolation

Private sources, contributed host machines, market account systems and youth learning environments must be isolated. Remote computing uses explicit grants and resource reservations with protection against uncontrolled networking, device actuation and secret leakage.

No automatic hardware driver access is conferred by a DataChip symbol name or a model suggestion.

Operations and incident response

Operators inspect job status, queue limits, integrity receipts, audit events and rollback paths through Command Centre. A failed or incomplete job does not generate a successful-use transaction. A revoked grant prevents new unauthorized work under the revoked authority.

Accurate incident reporting, system recovery, hardware diagnostics and independent checks protect users and preserve trust.

Rollout sequence

First establish source and identity contracts, then complete bounded repair, real native app rebuilding, host execution, distributed resource qualification, Bridge consent and Bit Trade Global usage accounting. Prove the integrated path against two materially different applications.

Make production claims for the particular supported feature only after its acceptance evidence exists.

SOURCES & PUBLICATION CONTROL

Blackmore Technology Group, BTG Universal Foundry cross-drive architecture and preservation review, 26 October 2026.

Blackmore Technology Group, consolidated Foundry engineering acceptance and source manifest, 26 October 2026.

Blackmore Technology Group, Building a Knowledge Capital Economy, October 2026 (historical edition).

https://www.blackmoretechgroup.com/universal-foundry.html

https://www.blackmoretechgroup.com/publications.html