UNITED KINGDOM INTELLECTUAL PROPERTY OFFICE

PATENT APPLICATION

Applicant

The Bitcoin Corporation Ltd

Title of Invention

The $402 Protocol: A Token-Based Micropayment System Using HTTP Status Code Signalling, URL Path Conventions, and Blockchain-Native Unilateral Contract Formation

Field of the Invention

The present invention relates to systems and methods for enabling native micropayments on the World Wide Web using the HTTP 402 "Payment Required" status code, blockchain-based tokens, and URL path conventions as payment signalling mechanisms. More particularly, the invention concerns a protocol that maps the HTTP 401, 402, and 403 status codes to distinct blockchain token layers for identity, payment, and permission respectively, creating a unified economic layer for web content and services that operates through standard web infrastructure without requiring additional software, plugins, or platform intermediaries.

Background of the Invention

Problem Statement

The monetisation of digital content and services on the World Wide Web has been constrained by fundamental architectural limitations since the web's inception:

1. The Unused Status Code — The HTTP 402 "Payment Required" status code was reserved in HTTP/1.1 (RFC 2616, 1997) for future use with a digital payment mechanism. Nearly thirty years later, no standardised protocol has been implemented to give this status code operational meaning. The web was designed to support native payments but the infrastructure was never built.

2. Advertising Dependency — In the absence of a native micropayment mechanism, the web's primary monetisation model became advertising. This creates perverse incentives: content is optimised for attention rather than quality, user data is harvested and sold, and a multi-billion-pound intermediary industry extracts value between creators and consumers.

3. Subscription Fatigue — The alternative to advertising — subscription paywalls — imposes binary access models (full access or no access) with high minimum price points. There is no mechanism for a user to pay a fraction of a penny for a single article, a single API call, or a single data query. The granularity of pricing is limited by traditional payment rails.

4. Identity-Payment-Permission Fragmentation — Modern web applications require three distinct functions: identifying the user (authentication), collecting payment (monetisation), and controlling access (authorisation). These functions are currently implemented through separate, incompatible systems — OAuth providers for identity, Stripe or PayPal for payments, and custom middleware for permissions. No unified protocol maps these three functions to a single, coherent framework.

5. Machine-to-Machine Payment Inability — As AI agents increasingly interact with web APIs on behalf of users, there is no standardised mechanism for an autonomous software agent to discover a price, make a payment, and receive access without human intervention. Existing payment systems require human authentication steps (CAPTCHA, 3D Secure, manual card entry) that are incompatible with autonomous operation.

6. Content Creator Payment Complexity — Independent content creators wishing to charge for digital goods must integrate with payment processors, manage accounts, handle chargebacks, comply with PCI-DSS requirements, and accept fees of 2.9% plus fixed charges per transaction. These costs and complexities make micropayments (sub-penny to sub-pound) economically unviable through existing channels.

7. Lack of Payment Signalling Convention — There is no established convention by which a URL can signal to a client — whether human or machine — that the resource requires payment before the resource is requested. Clients must make a request and receive a rejection before learning that payment is needed, and the rejection provides no standardised information about price, payment method, or token requirements.

Prior Art Limitations

Web monetisation proposals (W3C Web Monetization API) provide streaming payments but require browser extensions and do not use standard HTTP status codes. Payment channel networks (Bitcoin Lightning Network) reduce transaction costs but operate outside the HTTP protocol layer and require separate connection establishment. Recent implementations of HTTP 402 (e.g., the x402 protocol by Coinbase, published May 2025) address payments in isolation but do not integrate identity or permission layers, do not define URL path conventions for payment signalling, do not establish unilateral contract formation through HTTP responses, and operate exclusively on account-based blockchains (Ethereum/Base) using stablecoin transfers rather than native token economies with algorithmic pricing.

No existing system combines HTTP status code mapping across identity, payment, and permission functions; a URL path convention for human-readable payment signalling; blockchain-native token economics with algorithmic pricing; DNS-based facilitator routing; and unilateral contract formation through standard HTTP responses in a unified protocol.

Summary of the Invention

The present invention provides a web payment protocol ("the $402 Protocol") comprising:

a. A URL path convention using the dollar sign character ("$") as a reserved signalling character within URL paths to indicate that the resource at that path requires payment, the dollar sign being a legal reserved character under RFC 3986;

b. A tripartite token system mapping the HTTP 401, 402, and 403 status codes to distinct blockchain token layers: $401 tokens for identity verification, $402 tokens for payment, and $403 tokens for permission and access control;

c. An HTTP 402 response specification that constitutes a machine-readable unilateral contract offer, comprising the price, the accepted token, the payment address, and the pricing model, such that payment by the client constitutes acceptance of the offer and creates a binding contract through performance;

d. An algorithmic pricing engine that computes token prices as a deterministic function of remaining token treasury, published via a standardised discovery endpoint, such that pricing is transparent, independently verifiable, and requires no centralised pricing authority;

e. A DNS-based facilitator routing mechanism using CNAME records to direct payment verification through intermediary services, enabling multi-chain payment acceptance without code changes to the content server;

f. A hierarchical path permission inheritance system whereby payment for a parent path (e.g., "example.com/$section") grants access to all child paths beneath it (e.g., "example.com/$section/$article-1", "example.com/$section/$article-2"), with each level of the path hierarchy operating as an independent token market;

g. A discovery protocol using a standardised endpoint ("/.well-known/x402.json") that exposes token metadata, pricing parameters, accepted payment methods, and facilitator endpoints, enabling automated price discovery by AI agents and client software.

Detailed Description of the Invention

1. System Architecture

The $402 Protocol comprises the following principal components:

1.1 The $ URL Path Convention

The protocol establishes a convention whereby the dollar sign character ("$") embedded in a URL path segment signals that the resource at that path requires payment. The dollar sign is a legal sub-delimiter character under RFC 3986 (Uniform Resource Identifier: Generic Syntax) and RFC 1738, and is explicitly permitted in URL paths alongside characters such as hyphen, underscore, period, and tilde.

The convention operates as follows:

1. **Payment Signalling** — Any URL path containing a "$" character indicates that the resource requires payment. For example: "example.com/$premium-article" signals a paid resource, whilst "example.com/free-article" does not.

2. **Human Readability** — The dollar sign is universally recognised as a currency symbol, providing an immediate visual signal to human users that the resource has an associated cost.

3. **Machine Parseability** — Client software, including AI agents, can inspect a URL prior to making a request and determine from the presence of the "$" character that payment will be required, enabling pre-emptive price discovery via the well-known endpoint.

4. **Hierarchical Markets** — Each "$" segment in a URL path creates an independent token market. For example, in "example.com/$section/$article", the "$section" level and the "$article" level each have their own token, price curve, and holder registry. Payment at a parent level grants access to all children beneath it.

1.2 The HTTP Status Code Token Mapping

The protocol maps three existing HTTP status codes to three distinct blockchain token layers, creating a unified identity-payment-permission framework:

HTTP 401 Unauthorized → $401 Identity Token. When a server returns HTTP 401, it indicates that the client has not established identity. The $401 token system provides on-chain identity verification through a chain of inscriptions linked to OAuth identity providers (GitHub, Google, LinkedIn, X/Twitter, Microsoft, and domain ownership via DNS TXT record). The $401 token functions as the identity layer of the protocol.

HTTP 402 Payment Required → $402 Payment Token. When a server returns HTTP 402, it indicates that the client must pay to access the resource. The $402 token is the native payment instrument of the protocol. The 402 response includes machine-readable payment instructions: price, token identifier, payment address, and pricing model. The client acquires and transmits $402 tokens (or other accepted tokens) to the server's payment address. The transaction itself serves as proof of payment — no separate verification oracle or indexer lookup is required.

HTTP 403 Forbidden → $403 Permission Token. When a server returns HTTP 403, it indicates that the client is identified and may have paid, but lacks specific permission to access the resource. The $403 token system provides granular permission management, enabling content creators to define access tiers, time-limited passes, role-based access, and transferable permission tokens.

The three tokens operate in sequence: 401 (who are you?) → 402 (can you pay?) → 403 (are you allowed?). This sequence mirrors the existing semantics of the HTTP status codes as defined in RFC 2616 and RFC 7235, but provides each code with a functional blockchain-based implementation for the first time.

1.3 The HTTP 402 Response as Unilateral Contract Offer

A central innovation of the protocol is the treatment of the HTTP 402 response as a unilateral contract offer under established contract law principles. A unilateral contract is a promise exchanged for an act: the promisor makes a promise in exchange for the promisee's performance of a specified act.

The $402 Protocol structures every HTTP 402 response as a unilateral offer comprising:

1. **The Offer** — The server's 402 response states: "Pay X amount in token T to address A and receive access to resource R." The terms are deterministic, computed algorithmically, and identical for all clients.

2. **Acceptance** — The client's act of transmitting payment to the specified address constitutes acceptance through performance. No explicit agreement, signature, or acknowledgement is required beyond the payment itself.

3. **Consideration** — The client provides payment (tokens or cryptocurrency). The server provides access to the resource plus any associated tokens.

4. **Performance** — Content delivery occurs immediately upon payment confirmation. The server detects the incoming transaction and grants access.

5. **Immutable Record** — The payment transaction is recorded on the blockchain, providing an independently verifiable record of the contract's execution.

This mechanism creates binding contracts through standard HTTP interactions without requiring terms of service agreements, click-wrap licences, or any form of explicit consent beyond the act of payment.

1.4 Algorithmic Pricing Engine

The protocol defines a deterministic pricing mechanism whereby the price of each token is computed algorithmically as a function of the remaining token treasury. As the treasury depletes through purchases, the price changes according to the declared pricing function. The specific pricing function is configurable by the content creator and declared in the discovery document. Supported pricing functions include, but are not limited to: fixed price, linear decay, logarithmic curves, square-root functions, and bonding curves.

The pricing model is fully transparent and computable by any client. No negotiation, auction, or human pricing decision is required. The price at any moment is a pure function of the remaining treasury, which is publicly observable on-chain. Any client can independently verify the current price by reading the treasury state and applying the declared pricing function.

This mechanism ensures that pricing is deterministic, auditable, and free from centralised control. The content creator selects the pricing function at token creation; thereafter, the price is governed entirely by the algorithm and the observable state of the treasury.

1.5 DNS-Based Facilitator Routing

The protocol introduces a facilitator routing mechanism using DNS CNAME records. A facilitator is a payment verification service that sits between the content server and the paying client, verifying payment receipt and relaying access grants.

The routing mechanism operates as follows:

1. **CNAME Configuration** — A content provider wishing to accept $402 payments creates a DNS CNAME record pointing a subdomain (e.g., "pay.example.com") to a facilitator service (e.g., "facilitator.path402.com"). No code changes to the content server are required.

2. **Multi-Chain Acceptance** — The facilitator service handles payment verification across multiple blockchain networks (BSV, Ethereum, Solana, Base). The content server need not implement any blockchain logic; it delegates payment verification entirely to the facilitator via DNS routing.

3. **Facilitator Independence** — Any party may operate a facilitator service. Content providers may switch facilitators by updating a single DNS record, with no code changes, no migration, and no vendor lock-in.

4. **Revenue Distribution** — The facilitator handles revenue splitting between the content creator and the facilitator operator according to basis-point allocations specified in the discovery document (e.g., 80% to creator, 20% to facilitator).

1.6 Discovery Protocol

All $402-compliant servers expose a standardised discovery endpoint at "/.well-known/x402.json" containing:

- The token identifier (e.g., "$example.com")
- The pricing model and current price
- The treasury balance and total supply
- Accepted payment methods and blockchain networks
- The facilitator endpoint URL
- Revenue distribution parameters
- The server's payment address for each accepted chain

This endpoint enables automated price discovery by AI agents and client software. An AI agent encountering a $-prefixed URL can query the well-known endpoint, determine the price and payment method, execute payment, and access the resource — all without human intervention.

1.7 Hierarchical Path Token Markets

Each "$" segment in a URL path creates an independent token market with its own supply, price curve, and holder registry. The hierarchy operates as follows:

1. **Site-Level Token** — "$example.com" represents a site-wide access token. Holding this token grants access to all $-prefixed paths on the domain.

2. **Section-Level Token** — "$example.com/$section" represents a section-specific token. Holding this token grants access to all content within that section.

3. **Content-Level Token** — "$example.com/$section/$article" represents a single piece of content. This is the most granular access level.

4. **Inheritance** — Payment at a higher level in the hierarchy automatically grants access to all lower levels. A holder of the site-level token need not purchase section or content tokens separately.

5. **Independent Pricing** — Each level has its own price curve. A site-level token may cost significantly more than a content-level token, reflecting the breadth of access granted.

2. Payment Flow

A typical $402 payment cycle proceeds as follows:

1. A client (human browser or AI agent) requests a resource at a $-prefixed URL.

2. The server returns HTTP 402 Payment Required, with headers and a JSON body specifying: the price in satoshis or other denomination, the accepted token identifier, the payment address, the pricing model, the remaining treasury, and the discovery URL.

3. The client queries the discovery endpoint ("/.well-known/x402.json") if additional metadata is required.

4. The client constructs and broadcasts a payment transaction to the specified blockchain network, sending the required amount to the server's payment address.

5. The server (or its facilitator) detects the incoming transaction. The transaction itself is the proof of payment — no separate API call, webhook, or verification step is needed.

6. The server returns the requested resource with HTTP 200 OK, optionally including any tokens earned by the client as part of the transaction.

7. The payment is recorded on the blockchain as an immutable record of the transaction, serving simultaneously as payment receipt, access credential, and contract evidence.

3. Token Economics

Each $402-compliant domain or path operates its own token economy. Tokens are minted as BSV-20 or BSV-21 tokens on the Bitcoin SV blockchain. The token economics are configured by the content creator through the discovery document and include:

• **Total Supply** — A fixed total supply of tokens (default: 1,000,000,000) for each token market. The supply is fixed at creation and cannot be increased.

• **Treasury** — Unminted tokens are held in a treasury. Purchases draw from the treasury at the algorithmically determined price. As the treasury depletes, the price increases.

• **Transferability** — Tokens are standard BSV-21 fungible tokens and can be freely transferred, traded, or sold on any compatible marketplace. Access rights travel with the token.

• **Revenue Distribution** — Revenue from token sales is distributed according to the basis-point allocation in the discovery document: a configurable split between the content creator (issuer) and the facilitator.

• **Reusability** — Tokens used for access may be returned to the issuer and resold, creating a circular economy. Alternatively, tokens may be held permanently as access credentials or traded on secondary markets.

4. Multi-Chain Payment Acceptance

Whilst the protocol's native token layer operates on the Bitcoin SV blockchain, the facilitator routing mechanism enables acceptance of payments across multiple blockchain networks. The facilitator verifies incoming payments on any supported chain and issues access grants to the content server.

Supported networks include BSV (primary, native token operations), Ethereum and Base (ERC-20 tokens, USDC), Solana (SPL tokens, USDC), and any additional chain for which a facilitator adapter is implemented.

The primary inscription and token record remains on BSV regardless of which chain the payment was received on. The facilitator records cross-chain payment references in the BSV inscription, creating a unified payment record anchored to a single chain.

Brief Description of Drawings

The following drawings would accompany this application:

- Figure 1 — System architecture diagram showing the $ URL convention, HTTP status code token mapping (401/402/403), discovery protocol, facilitator routing, and blockchain inscription layer, and their interconnections.
- Figure 2 — Payment flow diagram illustrating the sequence from client request through HTTP 402 response, price discovery, payment transaction, server verification, and content delivery.
- Figure 3 — HTTP status code token mapping diagram showing the relationship between HTTP 401, 402, and 403 responses and their corresponding $401, $402, and $403 blockchain token layers.
- Figure 4 — Hierarchical path token market diagram showing site-level, section-level, and content-level token markets with inheritance relationships.
- Figure 5 — Algorithmic pricing diagram showing token price as a function of remaining treasury, illustrating how deterministic pricing operates across different pricing functions.
- Figure 6 — DNS-based facilitator routing diagram showing CNAME configuration, payment verification flow, and multi-chain acceptance.
- Figure 7 — Unilateral contract formation diagram showing the HTTP 402 response as offer, payment as acceptance, and blockchain record as immutable contract evidence.
- Figure 8 — Discovery protocol endpoint structure showing the "/.well-known/x402.json" schema and its fields.

Initial Claims

Note: These claims are provided in sketch form for the purposes of establishing a priority date. Formal claims will be drafted and filed within 12 months in accordance with UKIPO rules.

Claim 1 — URL Payment Signalling Convention

A method of signalling that a web resource requires payment, the method comprising: (a) embedding a dollar sign character ("$") within a URL path segment to indicate that the resource at that path is subject to a payment requirement; (b) configuring a web server to return an HTTP 402 "Payment Required" response when a client requests a $-prefixed URL path without valid payment credentials; (c) including within the HTTP 402 response machine-readable payment instructions comprising at minimum the price, the accepted payment token or currency, and a payment address; wherein the dollar sign character functions as both a human-readable visual indicator of cost and a machine-parseable signal enabling automated price discovery prior to resource request.

Claim 2 — Tripartite HTTP Status Code Token System

A system for managing identity, payment, and permission on the World Wide Web using blockchain tokens, the system comprising: (a) a first token layer ("$401 token") mapped to the HTTP 401 status code, providing on-chain identity verification through a chain of blockchain inscriptions each linked to a verified identity provider; (b) a second token layer ("$402 token") mapped to the HTTP 402 status code, providing a native payment instrument for web resource access; (c) a third token layer ("$403 token") mapped to the HTTP 403 status code, providing granular permission and access control tokens; wherein the three token layers operate in sequence — identity, then payment, then permission — mirroring the semantic ordering of the HTTP 401, 402, and 403 status codes, and together forming a unified economic and access control layer for web resources.

Claim 3 — HTTP Response as Unilateral Contract Offer

A method of forming a binding contract through HTTP protocol interactions, the method comprising: (a) a server returning an HTTP 402 response containing deterministic, algorithmically computed terms comprising the price, the payment address, the accepted token, and the resource to be delivered; (b) the terms being identical for all clients requesting the same resource at the same treasury state, with no negotiation or variation; (c) a client transmitting payment to the specified address, the act of payment constituting acceptance of the offer through performance; (d) the server delivering the resource upon detecting the payment transaction; (e) the payment transaction being recorded on a blockchain as an immutable record of the contract's execution; wherein the HTTP 402 response constitutes a unilateral contract offer and the client's payment constitutes acceptance, creating a binding agreement without explicit consent, signature, or terms-of-service acknowledgement beyond the act of payment itself.

Claim 4 — Deterministic Algorithmic Token Pricing

A method of pricing access tokens for digital resources, the method comprising: (a) establishing a fixed total token supply for a given resource or resource hierarchy; (b) maintaining a treasury of unminted or unsold tokens; (c) computing the price of each token algorithmically as a function of the remaining treasury supply, such that the price is deterministic and changes as the treasury depletes; (d) publishing the current price, the treasury balance, and the pricing function identifier via a standardised discovery endpoint, such that any client can independently compute and verify the current price without querying the server; wherein the pricing requires no centralised pricing authority, no negotiation, and no human intervention; the price at any moment is a pure function of

publicly observable on-chain state; and the pricing function is declared in the discovery document and may be any deterministic algorithm agreed upon by the protocol, including but not limited to linear, logarithmic, square-root, or bonding curve functions.

Claim 5 — DNS-Based Payment Facilitator Routing

A method of routing payment verification for web resources using DNS infrastructure, the method comprising: (a) a content provider creating a DNS CNAME record pointing a designated subdomain to a payment facilitator service; (b) the facilitator service receiving and verifying payment transactions across one or more blockchain networks on behalf of the content provider; (c) the facilitator service issuing access grants to the content server upon successful payment verification; (d) the content provider being able to switch facilitator services by modifying a single DNS record, without any code changes to the content server; wherein the DNS infrastructure serves as a decentralised routing layer for payment verification, enabling multi-chain payment acceptance through standard web infrastructure.

Claim 6 — Hierarchical Path Token Markets

A system for creating hierarchical token markets within URL path structures, the system comprising: (a) each dollar-sign-prefixed segment in a URL path constituting an independent token market with its own token supply, price curve, and holder registry; (b) a permission inheritance mechanism whereby holding a token at a parent path level grants access to all child paths beneath it; (c) independent pricing at each level of the hierarchy, such that site-level, section-level, and content-level tokens each have distinct prices reflecting the breadth of access granted; wherein the URL path structure itself defines the token market hierarchy, and access rights cascade from parent to child without requiring separate token purchases at each level.

Abstract

A web payment protocol ("the $402 Protocol") that implements the HTTP 402 "Payment Required" status code as a functional micropayment system using blockchain tokens and URL path conventions. The protocol establishes the dollar sign character in URL paths as a human-readable and machine-parseable payment signal. Three blockchain token layers ($401, $402, $403) are mapped to the HTTP 401, 402, and 403 status codes respectively, providing a unified identity-payment-permission framework. HTTP 402 responses are structured as unilateral contract offers, with payment constituting acceptance through performance. A deterministic algorithmic pricing engine computes token prices as a function of remaining treasury, published via a standardised discovery endpoint. DNS CNAME records route payment verification through facilitator services, enabling multi-chain payment acceptance without code changes. Hierarchical URL paths create nested token markets with permission inheritance. A standardised discovery endpoint enables automated price discovery by AI agents and client software.

Document prepared for UKIPO filing. Priority date to be established upon submission.

Applicant: The Bitcoin Corporation Ltd

Date of preparation: 28 February 2026