

CRYP2NOVA

Baseledger

PUBLIC-PERMISSIONED, COUNCIL GOVERNED NETWORK FOR ENTERPRISES

Whitepaper V1.0 - *(February 25, 2021)*

Marten Jung, Kyle Thomas, Stefan Schmidt, Ognjen Kurtic

baseledger.net

Archived copy · cryp2nova.com

Table of Contents

1 Abstract 3

2 Current State of Enterprise Blockchain 5

2.1 Enterprise Blockchain 5

2.2 Blockchain Initiatives 6

2.3 Industry Suitability and Use Cases 8

2.4 Enterprise Blockchain Types 12

2.5 The Baseline Protocol 15

3 The Problem: There is no “right” mainnet 20

3.1 Open Enterprise Challenges to be solved by a Mainnet 21

3.2 The Lack of a Unified Architecture for Multi-Chain Coordination 30

3.3 Problem statement 32

4 Solution: Baseledger as the Mainnet and Multi-Chain Coordinator 33

4.1 Architecture of Architectures 34

4.2 Consensus Model 36

4.3 Token Model 39

4.4 Council and Governance 49

5 Reference Implementation Examples 51

5.1 Phases and Process Flow of an Example Use-Case 51

5.2 Example Setups 53

5.3 Solution Details 56

6 Summary 63

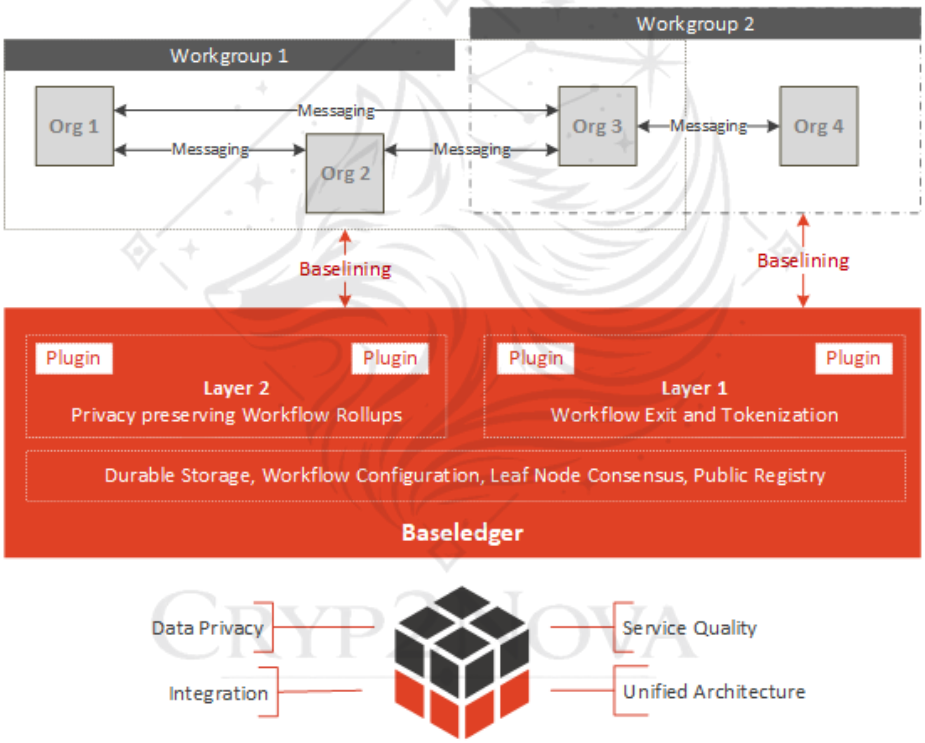
CRYP2NOVA

Archived copy · cryp2nova.com

1 Abstract

For a productive deployment of the Baseline Protocol across a variety of blockchain business cases at enterprise scale, the *right mainnet* is needed to coordinate Baseline-related consensus, configuration, and multi-chain setups.

- We present Baseledger: a public-permissioned, council-governed blockchain network that fulfills the major requirements of enterprise organizations for participating in Baseline-enabled processes: A unified architecture ensuring service quality, data privacy and integration.



We propose an *Architecture of Architectures*, introducing Baseledger as the underlying ledger for coordinating leaf node consensus, configuration, public DID registries and protocol interoperability enabling workflow exits and tokenization ("Layer 1") and privacy-preserving workflow and workstep rollups under zero-knowledge ("Layer 2"). Baseledger can serve as the basic protocol to serve Layer 2 functionalities and act as Layer 1 by storing baselined proofs in the Baseledger network. Additionally, Baseledger always works as the underlying Ledger for coordinating any multi-chain setups, e.g., combining Baseledger with Ethereum for DeFi.

Archived copy · cryp2nova.com



Baseledger

The Blockchain for Baselining

Archived copy - cryp2nova.com

2 Current State of Enterprise Blockchain

2.1 Enterprise Blockchain

Blockchain[1] has, in recent years, been praised as a revolution in business technology. In the decade since the launch of Bitcoin as the first recognizable blockchain implementation, companies, regulators, fintechs and independent technologists have spent a myriad of hours exploring its potential. The resulting innovations have begun to reshape business processes in all domains.

Many successful projects have unlocked digital innovations that would simply not be possible without blockchain. Because blockchain supports a single, shared version of immutable truth amongst participants, it can be independently verified by each entity, with no single entity acting as the authority. Enterprise blockchain provides a much-needed boost to the trustworthiness and transparency of recorded transactions and business events.

Citing Gartner[2], blockchain's key innovation is that it *"eliminates all need for trust in any central or permissioned authority. Blockchain introduces a new route to accelerate the move to digital business. This allows enterprise technology and innovation leaders to create or represent assets in a digital context and to create a new, decentralized economic and social model."*

CRYP2NOVA



Baseledger supports enterprise blockchain as a pillar in digital transformation. It supports evolutionary and incremental improvements in trust and transparency across business ecosystems. This enhances and supports the efficiency, auditability and trustworthiness of existing multiparty business processes, where no single party is in control.

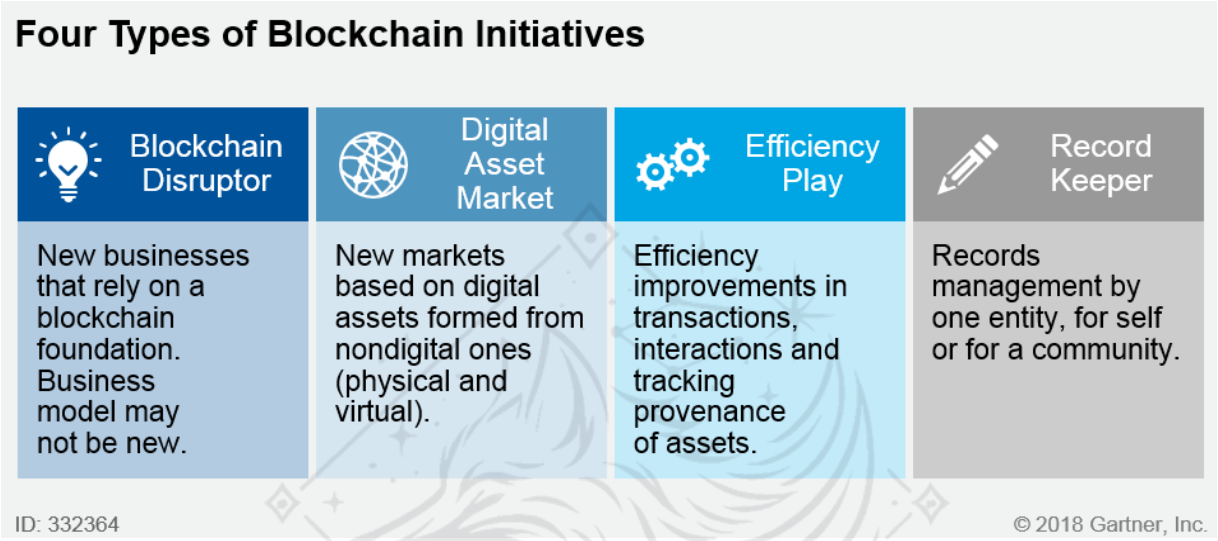
[1] A blockchain is a growing list (ledger) of cryptographically signed, irrevocable transactional records shared by all participants in a distributed network. Each record comprises a time stamp and reference links to previous transactions. With this information, anyone permissioned can trace back a transactional event, at any point in its history. A blockchain is one architectural implementation of the broader idea of distributed ledgers

[2] Gartner Research, Blockchain Unraveled: Determining Its Suitability for Your Organization, Published: 20 May 2019, ID: G00387734

Archived copy · cryp2nova.com

2.2 Blockchain Initiatives

Gartner[3] looked at blockchain initiatives adopted by startups, big companies, market infrastructure companies and others, spanning various industries and jurisdictions. For each initiative, the value drivers for blockchain were determined. Gartner's model for the four types of blockchain initiatives is the result of this research:



The four types of blockchain initiatives meet the needs of most businesses and encompass both cost-saving and revenue-generating initiatives. These initiatives can be seen in all types of organization, including commercial startups, consortiums, and individual enterprise and government projects. An organization is not limited to one type of initiative, described in further depth below:

- **Blockchain disruptor initiatives** rely primarily on a blockchain foundation to achieve decentralization of business and/or technology functions. Their critical business functionality is primarily enabled by the capabilities of blockchain, including the distributed ledger, strong consensus mechanism, immutability and traceability of records, and acceptance of cryptocurrencies.

- **Digital asset markets** involve new markets that stem from the creation (or representation) and trading of new digital assets using blockchain's cryptocurrency

[3] Gartner Research, Pay Attention to These 4 Types of Blockchain Business Initiatives, Published: 19 March 2018, ID: G00332364

Archived copy · cryp2nova.com

mechanisms. Digital asset markets tend to use all the value drivers of blockchain, including its ability to create/represent digital assets.

■ **Efficiency plays** attempt to improve efficiencies in existing business processes within a company or at an industry level. They usually preserve current business models and actors, with decentralization only implemented at the technology architecture level, if at all. In these initiatives, there are no new markets such as those created in the digital asset market initiative. Blockchain is only used to record transactions and events; that is, it is not used to facilitate them. The key value drivers of blockchain for these initiatives are the distributed ledger and the immutability and traceability of records.

■ **Record keeper initiatives** have a primary purpose, which is to ensure that records cannot be corrupted and that they can be audited on demand. Solutions can be private, benefiting just individual organizations, or shared, providing a common service for multiple organizations.



Baseledger is designed for all of these initiatives, driving value for all types of organizations.

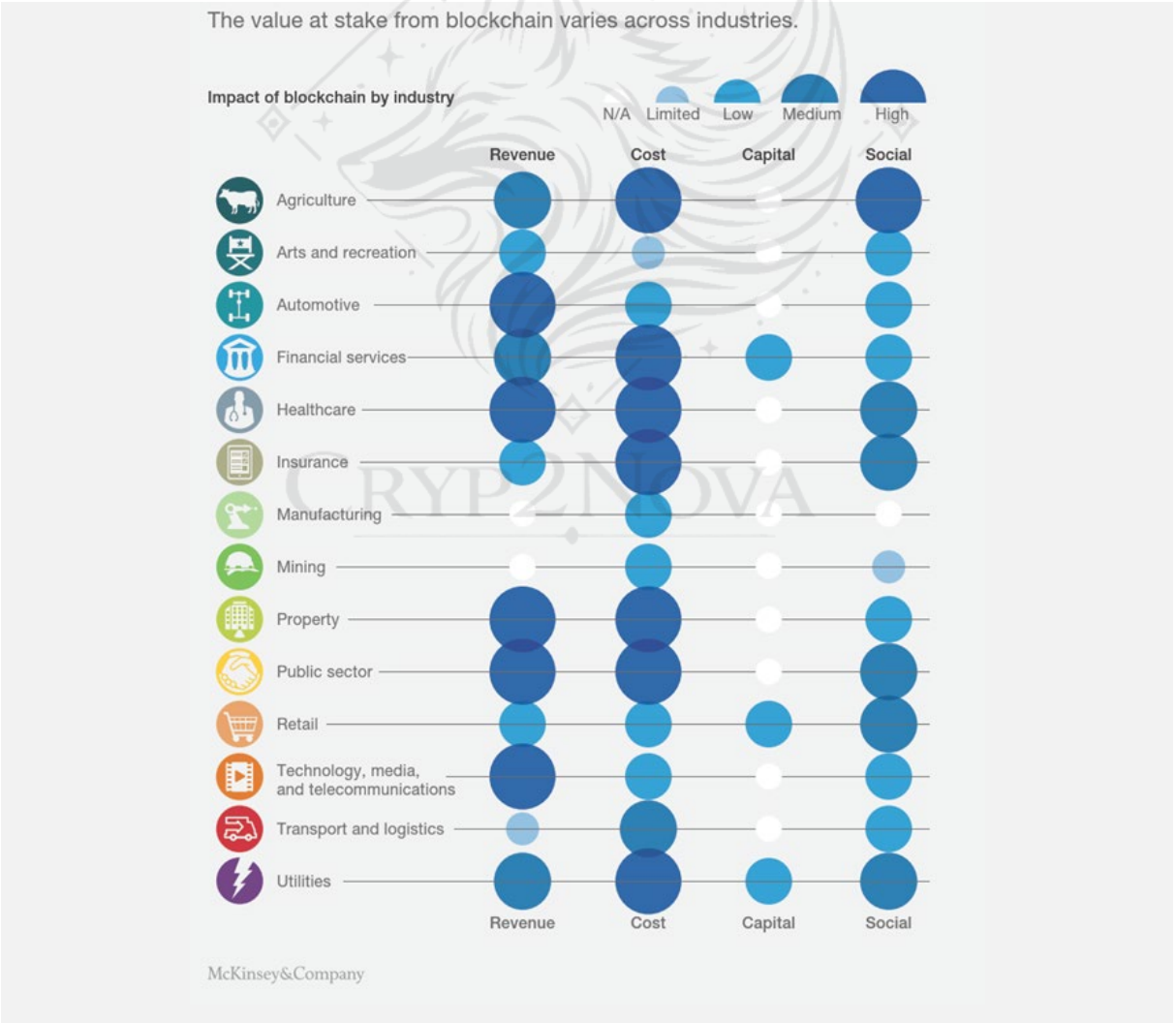
CRYP2NOVA

Archived copy · cryp2nova.com

2.3 Industry Suitability and Use Cases

Before implementing blockchain solutions, enterprises would be well-cautioned to check for two things: First, is there a valid business case (i.e. do any of the four initiatives fit)? Second, is blockchain the right solution, considering the business model, required process change, and maturity and enterprise-suitability of the given case?

Certain industries' fundamental functions are inherently better-suited to benefit from blockchain solutions; the financial services, government, and healthcare sectors capture the greatest value according to McKinsey&Company[4]. Based on the quantification of the monetary impact of the more than 90 use cases analyzed, it has been estimated that approximately 70 percent of the value at stake in the short term is in cost reduction (see "Efficency Plays"), followed by revenue generation and capital relief.



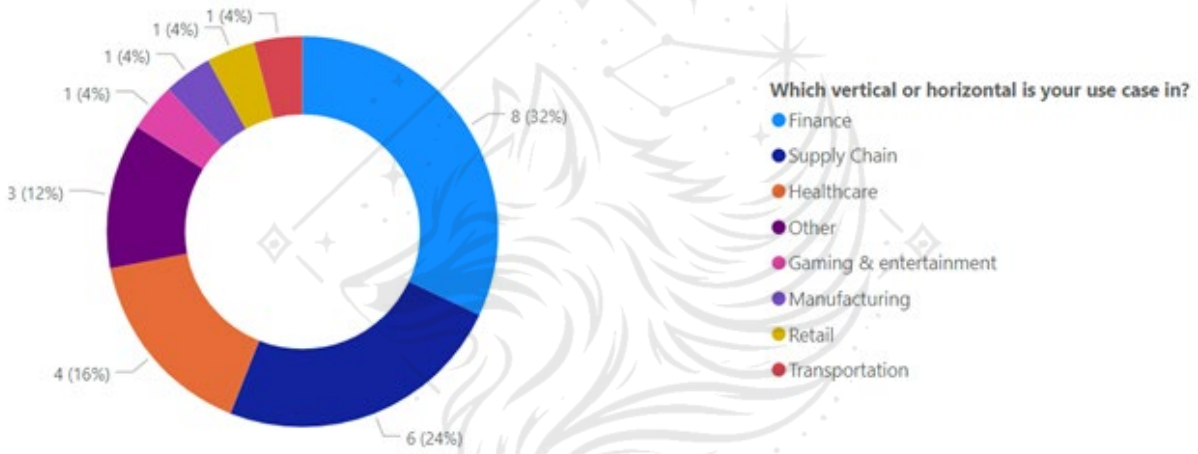
[4] McKinsey&Company, Blockchain beyond the hype: What is the strategic business value? Copyright 2018, Brant Carson, Giulio Romanelli, Patricia Walsh, and Askhat Zhumaev

Archived copy · cryp2nova.com

2.3.1 Use-Cases

The EEA Mainnet Working Group[5] created a task force in early 2020 to research enterprise use cases for Ethereum and identify the main pain points for adoption. As part of their work, they created a use case survey[6] that consisted of a questionnaire with topics such as use cases, challenges of building on the Ethereum Mainnet, benefits, performance requirements etc. The survey was active for a period of two months and gathered the following results:

"Finance, healthcare, and supply chain were the most frequently mentioned industries."



The primary challenges of blockchain adoption, as identified by survey participants, were:

- (Technology) Noisy neighbor, speed and latency
- (Compliance) Data locality problem
- (Business) Private data problem, gas costs, difficulty holding ETH

The primary benefits of building on the mainnet were:

- Security/Immutability
- Potential for interoperability with other applications, network effects
- Transparency of public chain

[5] https://entethalliance.org/participate/working_groups
[6] https://entethalliance.org/wp-content/uploads/2020/07/EEA_MWG_Survey-v1.pdf

Archived copy · cryp2nova.com

In terms of performance requirements, most participants did not have specific thresholds and from those who did, there was significant variation, from ~95%+ finality within 15-20 seconds to 8,100 transactions per minute.

The conclusions of the study were that security and interoperability are the main benefits of building against a common frame of reference such as the Ethereum Mainnet and that some of the challenges identified (i.e. Data locality) cannot be addressed by L1 and must be addressed in the upper layers in order for adoption to become viable. Also, based on the input related to scalability and performance, the study concluded that participants are currently focusing on the low-throughput application, since they are aware that the Mainnet cannot support use cases requiring high throughput at present. Participants also identified a number of challenges, such as the noisy neighbor problem (at the top of the list) that cannot be solved by L1 due to the design of Ethereum and that must be tackled in L2.

2.3.2 Integration

A key issue in all enterprise blockchain use cases is successful integration into existing IT system landscapes, which has been described by the *Eminen*t EEA Integration Taskforce, (which operates under the Ethereum Mainnet Working Group[7]). Although the scope of this taskforce revolves around Ethereum as the mainnet, the integration tasks are valid for all enterprise-related blockchain use cases:

- **Getting enterprises ready for mainnet** (process integration): This includes identifying processes or partial processes that can benefit from using blockchain. It includes identifying and defining the process or workflow steps that are handled off-chain and could be handled on-chain, for example exchanging quotes on a Request for Quotation process. This answers the question "*What could I use the mainnet for?*"

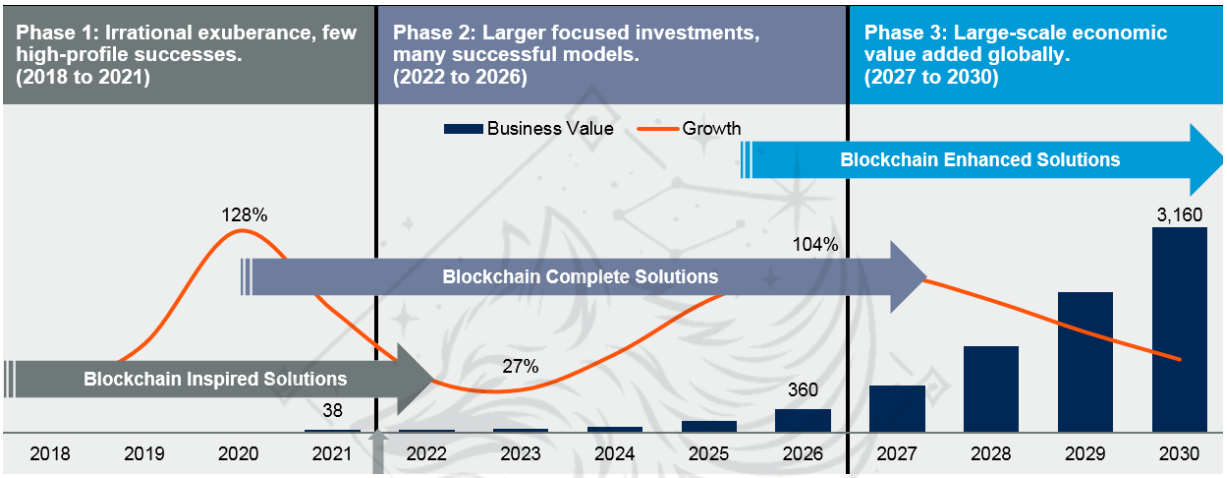
- **Getting mainnet ready for enterprises** (technical integration): This includes understanding the IT system landscapes that are already in place and building standards on how they should interact with the mainnet. The task is not so much about

[7] https://entethalliance.org/participate/working_groups

Archived copy · cryp2nova.com

specific processes, but rather about ground-laying technical integration which answers the question *"How do I connect to the mainnet?"*.

The below forecast by Gartner[8], which illustrates the business value of blockchain use cases, portrays a measured evolution on the business value of blockchain use cases. The belief is that little business value will be generated in the next five years. However, by 2025, the value added by blockchain will grow to a little more than $176 billion, then rush to exceed $3.1 trillion by 2030.



Baseledger is designed to support a variety of uses cases, without technical or architectural limitations to specific verticals. Integration as a key issue to all use cases is included in the core of the Baseledger Architecture of Architectures.

[8] Gartner Research, Predicts 2019: Blockchain Business, Published: 13 December 2018, ID: G00374378

Archived copy · cryp2nova.com

2.4 Enterprise Blockchain Types

2.4.1 Public / Permissionless Blockchains

Public (or permissionless) blockchains are decentralized systems designed to run transactional programs that access a fully replicated immutable data store without the need to have full trust in any single participant or in a third-party. Anyone can join the system by simply running a local instance of the corresponding peer-to-peer protocol.

The first permissionless blockchains were Bitcoin and Ethereum. They both constitute decentralized payment networks that introduce their own cryptocurrency and achieve probabilistic consensus (on which transactions have been executed in the current epoch, i.e., a "block" in which order) via protocols based on Proof-of-Work (PoW). Furthermore, to ensure the integrity and non-repudiation of these transactions, they utilize digital signatures.

Therefore, users can be identified in the network using their public keys without the need for real-world identities, which makes them pseudonymous. These systems favor absolute decentralization over privacy and performance, thereby enabling cryptocurrencies, which are their primary use-case. Thus, to a certain degree, they are only suitable for demanding, competitive or mission-critical use cases, such as most enterprise applications.

CRYP2NOVA

2.4.2 Permissioned Blockchains

Permissioned blockchains guarantee data confidentiality and ensure better performance at the expense of decentralization. Permissioned blockchains are blockchain systems in which participation is restricted. This includes systems in which all roles are restricted, such as *Hyperledger Fabric,* and systems in which only nodes (which participate in the consensus process) are restricted while other roles remain unrestricted.

Permissioned blockchains are suited for competing enterprises that are, nonetheless, willing to engage in collaborative processes without employing third-parties.

Archived copy · cryp2nova.com

Permissioned blockchains provide enhancements over their permissionless counterparts that facilitate enterprise-grade use cases:

i. Since the participation in the consensus protocol is limited to a specific group of users that requires explicit system reconfiguration to be modified, permissioned blockchains are able to use Byzantine Fault Tolerant (BFT) protocols, which offer improved transaction latency and throughput.
ii. Furthermore, permissioned blockchains offer greater confidentiality since sensitive transactions can be isolated from public access.
iii. Finally, permissioned blockchains can achieve transaction finality and other desirable transactional properties which their permissionless counterparts cannot. It is important to mention that enterprises still need permissionless blockchains, e.g., to utilize cryptocurrencies or store immutable hashes of confidential data for auditing purposes.

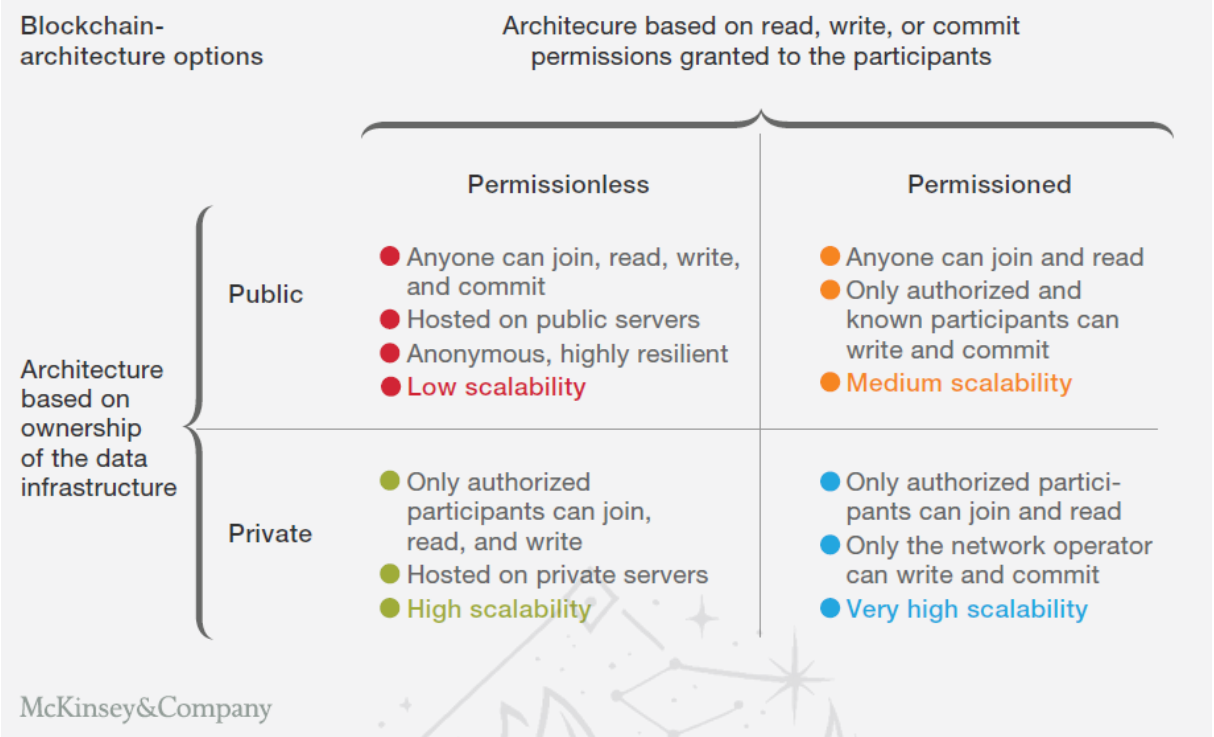
2.4.3 Public vs. Permissioned

Permissionless blockchains suffer from several drawbacks due to their fully replicated open nature and consensus mechanism:

- Low performance in terms of transaction throughput;
- High cost-per-byte in terms of data storage;
- Confidentiality issues because data is publicly-accessible on fully-replicated pseudo-anonymous nodes;
- Public blockchains never reach absolute finality because PoW allows forks (for example, due to network latencies); this lack of finality can result in certain transactions which were committed to the chain might and be revoked as a result of such a fork;
- Unpredictable costs are inherent to Proof-of-Work consensus mechanisms, as it is not possible to foresee how much a transaction will cost in the future; by extension, it is not possible to foresee how much a specific implementation will cost in the future.

According to McKinsey&Company , most commercial blockchain projects will use private, permissioned architectures.

Archived copy · cryp2nova.com



Although permissioned blockchains mitigate many major shortcomings of permissionless blockchains, they introduce a separate set of pain points for enterprise-grade applications:

- They add counter-productive centralization to the decentralized nature of blockchains
- Every participant must run a node, which is costly and complex (whereas permissionless blockchains which can be used in an ad hoc, pay-per-use manner
- For every (business) network or use case a new blockchain must be set up and maintained (1:1 dilemma)
- Permissionless blockchains are still needed, e.g., to utilize cryptocurrencies

Baseledger is designed to leverage the advantages of public permissioned blockchain networks to address the major needs of enterprises.

Archived copy · cryp2nova.com

2.5 The Baseline Protocol

2.5.1 The idea of the Baseline Protocol

The Baseline Protocol[9] creates the opportunity for compelling enterprise blockchain solutions by addressing core demands for enterprises looking to use blockchain technology: privacy, permission, and performance. It combines the advantages of public and private blockchains while mitigating their respective drawbacks.

EY and ConsenSys announced the formation of the Baseline Protocol in March of 2019 in collaboration with Microsoft as an open-source initiative. Unibright and Provide are among the founding members of the Baseline Technical Steering Committee and each has played a significant role in the design and architecture of the Baseline Protocol and production-ready reference implementation while also serving the community in leadership and governance roles.

The Baseline Protocol is an approach to using a public blockchain (i.e., a mainnet) as the common frame of reference between disparate distributed systems, including traditional corporate systems of record, databases, state machines or even different blockchains. Baseline is a particularly promising way to reduce capital expenses and other overhead while increasing operational integrity when automating interorganizational business processes and data sharing.

CRYP2NOVA



Baseline – synchronizing off-chain systems of record on a public blockchain

[9] http://baseline-protocol.org/

Archived copy · cryp2nova.com

The Baseline Protocol enables confidential and complex collaboration between enterprises without sharing sensitive data on-chain. It enables the execution of workflow business logic under zero-knowledge. It supports tokenization and DeFi while leaving enterprise data safely in traditional systems with zero impact on end users.

Participants in a business process, such as subsidiaries or business partners (like subcontractors) collaborate under various agreements, but may struggle to verify or reconcile those agreements — in other words, to trust that terms and conditions that have already been agreed upon are actually followed. Baseline enables trust among organizations which otherwise have no reason to trust one another by using a public blockchain to store relevant proofs, while leaving sensitive business data off-chain.

2.5.2 Example Use-Cases and Proof-of-Concepts

CONA (Coke One North America)

In partnership with CONA Services (Coke One North America), Provide and Unibright are working on baselining the Coca-Cola Bottling Supply Chain in North America[10]. In 2019, the first set of CONA Bottlers adopted a blockchain platform based on Hyperledger Fabric, which runs on SAP's Blockchain-as-a-Service (BaaS) platform. CONA is now extending this use case from an internal network to a larger audience utilizing the Baseline Protocol. The goal of the initiative is to establish a "Coca-Cola Bottling Harbor," offering a low barrier to entry for additional Coca-Cola bottlers. The Harbor will benefit not only internal CONA bottlers, but also external bottlers and their suppliers (e.g. raw materials vendors supplying cans and bottles), who will have access to a private, distributed integration network and DeFi-native invoice factoring.

The project is using the Baseline Protocol and technology stack built by Provide and Unibright to combine the advantages of permissioned and permissionless blockchain networks with the Baseline Protocol design pattern. Still, with the use of Ethereum as the public mainnet, there are ongoing discussions regarding its highly unpredictable performance and cost structures.

[10] https://medium.com/unibrightio/baselining-the-north-america-coca-cola-bottling-supply-chain-f87539220269

Archived copy · cryp2nova.com

Fraunhofer IPK

Together with Fraunhofer IPK, Unibright and Provide are collaborating on baselining additive manufacturing[11]. A blockchain demonstrator for an additive manufacturing plant that is available at the Fraunhofer IPK and based on Hyperledger Fabric has been adapted to the guidelines of the Baseline Protocol and expanded to include integration into SAP. Through joint research activities, the potential of the Baseline Protocol for the manufacturing industry has been shown. In follow-up projects, common standards for the use of Baseline in Industry 4.0 and IoT are to be developed together with manufacturing companies.

One key question — especially in relation to IoT — is which platform can support up to billions of devices from a performance, cost, and data ownership perspective? In integrated manufacturing, there is ongoing discussion on how to integrate blockchain systems with surrounding off-chain systems like SAP and various Microsoft ERP systems.

Between

This collaboration between Serbian blockchain factoring startup Between.rs, Unibright, and Provide explores baselined invoice tokenization with Between factoring platform finspot.rs[12]. Off-chain integration leveraging zero-knowledge proofs enable the provenance of an invoice to be verified prior to workflow exit; upon exit, qualifying invoices are tokenized. After tokenizing the invoice, it can be considered a financial instrument which can be sent to a lending facility for inclusion in a tranche or pool of collateralized assets categorized by type and risk.

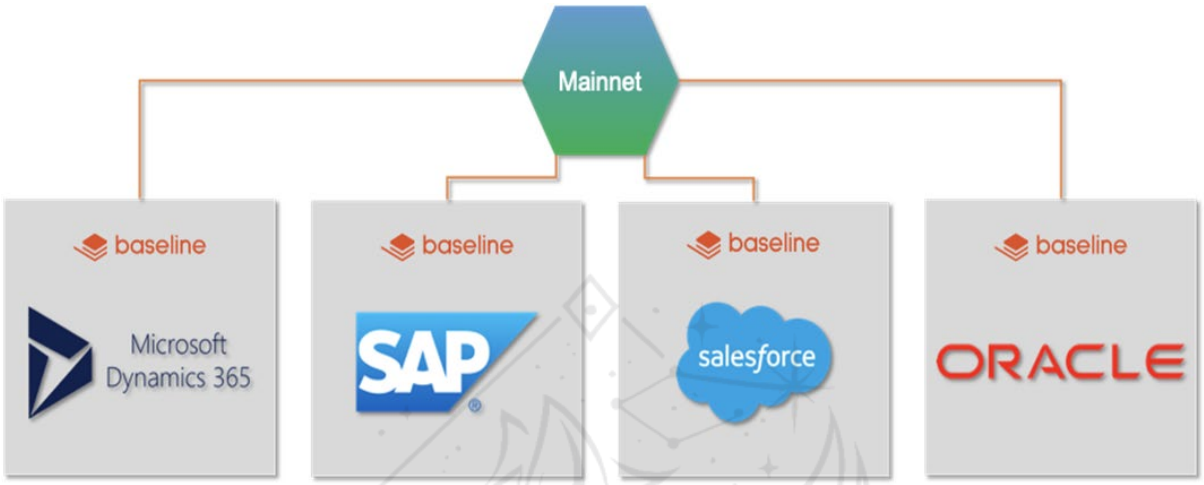
Baseline amplifies the value chain to the benefit of the parties that can then extract it without compromising the privacy of any counterparty. In other words, a factoring company can tokenize an invoice without knowing any details about the parties involved. The Baseline Protocol enables investors to verify a transaction happened and that a credit risk assessment has indicated the transaction is suitable for tokenization. The investor thus knows that his/her money is invested in a rated financial instrument and that the projected returns are sound.

[11] https://medium.com/unibrightio/unibright-and-fraunhofer-ipk-collaborate-on-baselining-additive-manufacturing-7469c36143a3
[12] finspot.rs

Archived copy · cryp2nova.com

2.5.3 The Mainnet

A business process is considered *baselined* when two or more systems store data and run business logic in a verified state of consistency, enabled by using a mainnet as the common frame of reference.



A "mainnet" in the context of the Baseline Protocol[13] is an always-on public utility — serving as a state machine — that sacrifices speed, scalability and fast finality for tamper- and censorship-resistant consensus. Because the mainnet is a permanent public ledger, any encrypted information recorded there can be observed by anyone at any time, forever. This includes parties with the means and know-how to perform advanced analytics, identifying patterns that may reveal strategic intelligence without even decrypting the data itself.

Implemented correctly by design, the mainnet can be used in global business to solve long-standing synchronization and consistency problems by:

1. Automating commercial agreements without creating new silos (e.g., like private blockchains do);
2. Democratizing ecosystem access and inclusion without losing system integrity or adding fragmented integrations;
3. Enforcing verifiable consistency between different parties' records without moving the data or business logic from legacy systems and without impacting end users;

[13] https://docs.baseline-protocol.org/baseline-protocol-standard/standards/mainnet

Archived copy · cryp2nova.com

4. Enforcing consistency in a multiparty workflow (e.g. invoices always agree with the purchase orders) while compartmentalizing which parties know the details of each step

Of course, one can attempt to accomplish these same goals using a centralized portal or platform, provided he/she does not mind (a) bearing all the cost of setting up and running the portal, (b) forcing all counterparties to use it and (c) sharing privileged information with the portal operator, who might become compromised or have malicious intentions. Network effects are powerful — they should not be underestimated.

The key to the Baseline approach is to memorialize workflow exit and tokenization on a public blockchain under zero-knowledge while ensuring off-chain state transitions which "rollup" prior to exit are sufficiently entangled. This design mitigates the aforementioned risks without introducing lock-in to create significantly more inclusive, efficient enterprise ecosystems.

The Ethereum public network is, as of December 2020, the chosen candidate to serve as the common frame of reference for distributed systems implementing the Baseline Protocol. However, according to the official Baseline docs[14], *"it still should be observed that the requirements, not any particular formulation or named service today, are the essential thing. That said, if there is a platform that better matches these specs today, and is more likely to evolve from a position of critical mass (achieved by Ethereum at a key historical moment in 2015) to meet the world's expanding use of it, that platform should step up now."*

CRYP2NOVA



Baseledger is designed to support the Baseline approach, enabling a production ready mainnet architecture at enterprise scale as outlined in the Baseline Protocol.

[14] https://docs.baseline-protocol.org/baseline-protocol/the-baseline-protocol [Section "Which Mainnet"]

Archived copy · cryp2nova.com

3 The Problem: There is no "right" mainnet

As explained, the Baseline Protocol — and with it the approach to baselining — already outlines how to overcome the private versus public discussion: by using a public blockchain to establish trust, while keeping private business data on off-chain systems.

Ethereum, the frontrunning candidate for a Baseline mainnet, is facing numerous challenges. The severity of these challenges is indicated by the number of individuals and organizations attempting to address them, such as the Enterprise Ethereum Alliance and even the Ethereum Foundation itself:

- Scaling problems
- Speed and latency problems
- Finality problem
- Noisy neighbor problem

The referenced document[15] discusses these problems by comparing Layer 2 solutions with "Baseline" solutions, but does not discuss the suitability of Ethereum itself as the Mainnet within Baseline. In such a competitive area, it is very likely that different blockchain networks will attempt to position themselves as a candidate mainnet, as evidenced by the uptick in interest from public-permissioned blockchains[16].

CRYP2NOVA

Baseledger tackles the obvious challenge to find or build the right mainnet for Baseline applications.

[15] https://entethalliance.org/how-ethereum-layer-2-scaling-solutions-address-barriers-to-enterprises-building-on-mainnet
[16] https://hedera.com/blog/unibright-integrates-hedera-token-service-to-scale-asset-tokenization

Archived copy · cryp2nova.com

3.1 Open Enterprise Challenges to be solved by a Mainnet

Distilling the learnings from the example use cases and PoCs previously discussed, and including results from the EEA Use Case and Integration Task Forces, three vital enterprise challenges for blockchain adoption have been identified: *Service Quality*, *Data Privacy*, and *Integration*. They must be addressed to enable widespread enterprise usage of the Baseline approach for distributed business processes in terms of a mainnet.

Service Quality represents the broadest field, applicable to all business services. We will present the *Service Measurement Index* as the criteria catalog for this field. *Data Privacy* demands special treatment due to the unique nature of blockchain technology. *Integration* covers the technical integration of business IT system landscapes, blockchain-specific integration tasks, and the integration of additional business processes.

3.1.1 Service Quality

The *Service Measurement Index* ("SMI")[17] was designed based on International Organization for Standardization (ISO) standards. It consists of a set of business-relevant Key Performance Indicators (KPIs) that provide a standardized method for measuring and comparing business services.

The SMI framework provides a holistic view of Quality of Service (QoS) needed by customers for selecting business services (including blockchain services) to evaluate the feasibility of an enterprise solution based on:

- **Costs**: Is the service cost-effective (per transaction, data storage, integration,…)?
- **Performance**: Are there predictable projections for usage of service in terms of performance metrics?
- **Accountability**: Are there concepts in place to serve demands around governance, support and service level agreements?
- **Agility**: Is the service elastic, portable, adaptable and flexible?

[17] Cloud Services Measures for Global Use: The Service Measurement Index (SMI), Published in: 2012 Annual SRII Global Conference, Jane Siegel; Jeff Perdue

Archived copy · cryp2nova.com

- **Assurance**: Will the service perform as expected (reliability, resiliency and service stability)?
- **Usability**: Is it easy to integrate the services into the existing landscape (Accessibility, Installability, Learnability, Operability)?
- **Sustainability**: Can it be assured that the different technical components of an enterprise solution can be maintained, enhanced or (if needed) exchanged without affecting the overall availability of the solution?

3.1.2 Data Privacy

The regulatory landscape for data privacy changed in 2018 with the European Union's sweeping General Data Protection Regulation (GDPR) coming into effect[18]. Data privacy regulations — GDPR included — are often seen as counter-intuitive and difficult to align with the permissionless, distributed, and immutable nature of public ledgers. The incredible pace of change in terms of data privacy, as well as continued regulatory uncertainty among businesses and consumers, is still increasing. This holds true globally. For example, in the US, three states have passed personal data privacy legislation since 2018, including the California Consumer Privacy Act (CCPA), while many other states have data privacy bills moving through the legislative process.

These data privacy regulations share common principles and grant similar rights to the data subject. For example, both GDPR and CCPA bear the rights to correct, update, or delete data on a business database and require businesses to obtain consent for certain collection, processing, transfer, or sale of personal data. Software solutions, including blockchain-based ones, must be built in a way that considers these issues. Scrutiny over the way organizations manage data privacy rights has never been higher. Regulators have full-bodied enforcement agendas; consumers across the globe are learning how they can take action to protect their own data privacy; and enterprises, large and small, are tackling the operational, technical, and reputational challenges for business-as-usual operations. In parallel, significant uncertainty remains in how these data privacy regulations apply to blockchain technology.

It seems obvious for (enterprise) users of blockchain technology that data privacy matters warrant significant consideration. Especially from a legal perspective,

[18] https://eur-lex.europa.eu/content/news/general-data-protection-regulation-GDPR-applies-from-25-May-2018.html

Archived copy · cryp2nova.com

technology to be used within an enterprise ecosystem must follow specific regulatory demands that vary per jurisdiction.

Therefore, it is key to build a solution that is compliant with regulatory data privacy demands. Key challenges associated with reconciling data privacy regulations with DLTs are data mutability, data residency, and data democracy, which are covered in the following sections.

Data Mutability

Under the GDPR and other regulations, some data subject rights require the modification of previously collected data. For example, data subjects may have the right to correct inaccurate or outdated data, commonly referred to as the right of rectification, and the right to delete collected data. Blockchains are always described as an immutable or tamper-proof ledger or distributed database. This immutability is portrayed as a key enabler of the trust in the blockchain through resistance to malicious modifications. Once a transaction is added to a block and that block added to the end of the chain, then after some number of additional blocks are added, the transaction in question is effectively written in stone, as it would be impractical for an attacker to modify that transaction. Immutability appears to make it difficult or impossible to satisfy the requirements of the right of erasure, at least in regards to data stored on-chain.

The fundamental challenge for supporting a user's right to demand modification or erasure of their personal data if maintained on an immutable chain is not that it is impossible to delete a given piece of data, but rather that doing so would prevent subsequent validation of the chain. Specifically, the running hash would be invalidated if data was to be deleted.

Data Residency

On a typical public blockchain network, the network data is distributed and replicated across many geographically distributed nodes. Data privacy regulations often classify that protections may be rendered useless if the data is able to be freely transferred to another jurisdiction with less severe data privacy requirements. In the context of GDPR, for example, there are detailed requirements about the transfer of EU data to, or viewing of such data from, other jurisdictions. In general, the recipient of this data must

Archived copy · cryp2nova.com

be under a legally binding obligation to follow GDPR data protection principles or their equivalent.

Data Democracy

Data Democracy means information is controlled by those who generate it. This offers a more holistic view on data ownership, usage, and rights. It may sound straightforward, but in a world where personal and enterprise data is being exchanged with multiple parties, providers, governments, and others, this is a complex task.

■ Status Quo: Giant data silos and monopolistic control

Today, *cloud* is simply a slogan for data storage on someone else's computer. When the data is held in this centralized and siloed way by a third-party, users are exposed to threats such as censorship, surveillance and access restrictions which could impact their autonomy and decision-making. For example, in fall 2019, a modification in export law required that U.S. companies block users connecting from Syria, Iran, Venezuela, and Cuba[19]. Suddenly, users were unexpectedly unable to access their data. Some Silicon Valley business models rely on monopolistic control of user data and interaction. This is why approaches on data democracy haven't been pursued by many in the technology industry to date. User data is held hostage. It is sold to the highest bidder and not controlled by those who generate it.

■ Peer-to-peer networks

One way to overcome monopolistic data silos would be to host data on peer-to-peer networks, similar to BitTorrent, instead of a cloud or centralized server. This approach it does eliminate the centralization, but has shown to have major drawbacks. At first, there has to be one peer-to-peer connection for every relationship. Consider a complex supply chain with hundreds of involved parties – this would require thousands of individual connections to be maintained. Second, and potentially even worse is the lack of trust between parties. No one can be sure that their data is not being manipulated by the counterparty of a P2P connection – i.e., there is no way to prove data integrity.

[19] https://www.cfr.org/backgrounder/what-are-economic-sanctions

Archived copy · cryp2nova.com

(Classical) Blockchain

Blockchain technology seems to address these issues. It has proven to be a clever mechanism that facilitates transactions across a web of potentially untrusted computers. It also is a distributed system and uses some of the same computer science concepts as peer-to-peer applications. But blockchains need to have a consensus mechanism in place, because public transactions are mediated between participants which are all potentially malicious.

These trustless transactions are the key assumption baked within blockchains that distinguishes them from peer-to-peer applications. Most public blockchains, like Bitcoin and Ethereum, employ actors called “miners” for the consensus mechanism, who run computationally expensive algorithms in exchange for monetary compensation. This incentivizes the purchase of ever larger and more expensive data centers, rewarding miners who are able to take larger financial risks. In other words, the rich get richer.

Returning to the issue of data privacy, we see that this trend towards fewer, richer miners also leads to a centralized structure. There exists a famous picture taken a few years ago with less than 10 people on it, who represented about 90% of Bitcoin’s mining power! This handful of partly unknown and not-bound-to-any-contract miners could decide the fate of the Bitcoin network. For example, they had the power to manipulate transaction data or halt the network. In this early model, the only protections the network had against these kinds of "bad actors" were monetary incentives. It follows that these classical PoW blockchains are not suited for data storage or processing when data privacy is taken into account.

Although some blockchain proponents may claim Proof-of-work is ‘trustless’, technology is not neutral, which in practice means that you have to trust someone at some point. Within these classical blockchains, one doesn't know who processes and stores data, which rules and laws they follow (if any) or where and how the data is stored.

Archived copy · cryp2nova.com

3.1.3 Integration

Technical Business Integration

Citing David, Guy, & Vernadat[20], "business integration is the use of system architectural principles, software architecture and implementation to integrate a set of enterprise computer applications. It means the integration, automation and optimization of IT based business processes within and beyond the walls of a company's organization. In short, it is asking the question how enterprises can add blockchain solutions into their existing ecosystems."
The purpose of business integration may be data integration, abstraction from specific vendor systems (to ensure independence and integrity), or providing common front-ends and standardized queries on available data.

In demarcation of related terms, we understand business integration as one motivation to define (distributed) business processes[21] and implement (distributed) business workflows[22] on top of them.

There are commonly agreed challenges to business integration to be considered.

- **Message Exchange**: Within a business workflow, various parties need to exchange messages.
- **Notifications**: When a message is sent, the sender wants to make sure the message arrived. The recipient may need to inform the sender on missing information.
- **State Management**: Parties have to keep track of already sent messages and notifications.
- **Control Flow**: Workflows have to be enabled to react on different parameters changing, by defining control flow with elements like decisions, choices, loops or exceptions.
- **Changing Requirements**: Existing workflows have to be updated. Parties have to be added, system components may be changed and changes in established control flows may be introduced.

[20] C. David, D. Guy, and F. Vernadat, Architectures for enterprise integration and interoperability: Past, present and future, Computers in Industry, vol. 59, no. 7, pp. 647-659, 2008.
[21] A.-W. Scheer and M. Nuettgens, ARIS architecture and reference models for business process management. business process management, ed., 2000
[22] G. Mentzas, C. Halaris, and S. Kavadias, Modelling business processes with workow systems: an evaluation of alternative approaches. International journal of information management ed., 2001.

Archived copy · cryp2nova.com

- **Data Integrity**: Different message formats on different parties need mappings to ensure content integrity.
- **Technical Integrity**: Different channels, protocols and messages have to be orchestrated to keep all parties connected to the business integration process.
- **Security**: It has to be assured that the desired partner is reached, data holding information needs encryption and validation.

With blockchain technology being just one addition to the already diverse landscape of enterprise information technology, it is essential to integrate into existing systems. This holds true for "just" the technical connection of blockchain with traditional off-chain ERP and legacy systems.

More complex is the domain of business processes. Established and envisioned business processes using blockchain need to be designed and modelled by domain experts, which are rarely blockchain experts. Enterprises need tools that allow them to stay in the environment (the "domain") in which they have expertise and resources.

A complete vertical stack is needed, offering connectors to ERP Systems and usage of domain models that allow enterprise business process experts to stay in their domain.

Domain-specific APIs and tools that abstract from coding details and toolsets for distributing, deploying, running and monitoring ongoing business processes are needed. A high level of automation and abstraction enables a desired "integration maximum", where companies do not see or feel that they are using a new technology.

To achieve enterprise blockchain adoption, it is vital that solutions can be integrated out-of-the-box into the existing off-chain world, meaning the 99%+ of non-blockchain systems and processes already in place by companies worldwide.

Blockchain Specific Integration Tasks

Due to the nature of blockchain networks, there are specific demands that need to be addressed for enterprise usage. One discovered adoption is the involvement of native cryptocurrencies as a payment model for transactions costs on specific networks (e.g. "gas costs" to be paid in Ether for the Ethereum Blockchain).

Archived copy · cryp2nova.com

The usage of wallets, cryptocurrencies, and different blockchain ecosystems leads to a variety of sub-tasks, like key management, crypto value custody and compliant accounting.

Additional Services

As most blockchain networks implement a high level of pseudonymity, there is special attention to pay when identity management is needed or questions arise on data ownership, responsibility or permissions.

Identity management (i.e., being able to find out the identity of a participant if required by law enforcement) is the issue of Identity vs. Anonymity. Most often, the ability of users and operators of blockchain technology to stay pseudonymous is a core feature of the respective technology.

Nearly all blockchains have chosen extreme balances between user privacy and accountability. Some blockchains allow fully anonymous transactions without any accountability, making them vulnerable to illegal activity. Equally troubling is that while some blockchains do not provide true anonymity for transactions, allowing for transactions and accounts to be tracked, they offer no systematic way to discover the real-world identity of suspicious users.

Existing DLT solutions like Bitcoin and Ethereum significantly favor anonymity over known identity. With this design decision, these networks are in fact shying away from supporting the vast majority of corporate use cases. It is vital to point out that anonymity does not favor data protection or data privacy: not knowing who is processing what data is the opposite of data privacy and data protection.

However, for the majority of enterprise use cases, an anonymous environment may be undesirable for other reasons. Most business scenarios rely on knowledge of the involved parties. There should be a way for businesses to be able to verify the parties to a transaction to support legal enforcement of contracts. Data compliance frameworks like GDPR cannot work if data processors (node operators) can stay in total darkness.

Archived copy · cryp2nova.com

When leveraging the privacy promises of blockchain technology into an enterprise grade environment, a *phonebook-like registry* concept is another key issue to be handled. Identifying the business partner for an enterprise relationship must be done in a way whereby this registry does not conflict with the key features of the solution itself.

Baseledger is built around the main enterprise requirements for service quality, data privacy and integration.

Archived copy · cryp2nova.com

3.2 The Lack of a Unified Architecture for Multi-Chain Coordination

A key problem observed within the nascent enterprise blockchain space is the lack of a unified architecture that solves the scaling trilemma of blockchain while also delivering on its promise to organizations by encapsulating every rung in the value chain.

The reason for this is because a coordinated architecture capable of delivering the transformative value organizations are seeking requires multiple consensus protocols. **There is no one protocol which solves all needs.** This fact deserves additional attention when considering that enterprise solutions are built to last for years or even decades, while new blockchain protocols and standards are yet to be created.

When considering current public ledgers (mainnets) like Bitcoin or Ethereum, we can see that they primarily offer benefits for cryptocurrencies and their applications. These involve (pseudo)anonymity for users and node operators, but with no guarantees or standards for the network or its operators in terms of performance, location of the involved hardware, SLAs, transaction costs or support. As a result, they cannot be easily stopped by regulators or governments.

From a business perspective (that of a CIO, CTO or regulator) it becomes obvious that key aspects for cryptocurrency-focused ledgers contradict enterprise needs, for example:

- Guarantees on performance, availability and latency
- Fixed or at least predictable costs (e.g., per transaction, unit of storage, etc.)
- Clear commitment on data privacy and protection standards implemented (e.g., GDPR)
- Support guarantees and reliable SLAs (e.g., service level agreements)

These are not necessarily shortcomings of cryptocurrency DLTs — as compared to business DLTs — it is more that they serve different purposes and thus deserve different consideration in a unified architecture. Ethereum, for example, is not the obvious

Archived copy · cryp2nova.com

choice for a business mainnet, but a preferred candidate for handling cryptocurrencies, altcoins, and everything around DeFi, which may extend business processes.

From an architecture perspective, it is important that vendors providing commercially-supported Baseline-as-a-Service offerings have a clear interface highlighting how various infrastructure and software components can be implemented and loosely-coupled.

We understand "Layer 1 Protocols" as standards for workflow exit and tokenization, i.e. to provide notarized, "rolled up" states representing anonymized business processes, and "Layer 2 Protocols" as standards for privacy-preserving workflow and workstep state transitions which "rollup" prior to exit and are sufficiently entangled with previously-validated state.

It is clear that many bespoke Layer 1 and Layer 2 protocols exist today, but the efficacy of blockchain in the context of delivering enterprise value remains relatively low. Due to the cost and complexity of designing production-ready solutions that incorporate bespoke Layer 1 and fast-moving Layer 2 protocols, productive use of blockchain at enterprise-scale has remained inaccessible to organizations.

The Baseline Protocol is a significant breakthrough in communicating the benefits of blockchain to enterprise decision makers and promises to define a standard for interorganizational business process automation, but it also requires the aforementioned design decisions related to Layer 1 and Layer 2 consensus prior to adoption.



Baseledger supports a unified architecture, specific enough to serve the defined standards of the Baseline protocol, and sustainable enough to ensure future evolvement of different Blockchain protocols.

Archived copy · cryp2nova.com

3.3 Problem statement

For a productive deployment of the Baseline Protocol across a variety of blockchain business cases at enterprise scale, we need the right mainnet to coordinate Baseline-related consensus, configuration and multi-chain setups.



Archived copy · cryp2nova.com

4 Solution: Baseledger as the Mainnet and Multi-Chain Coordinator

We present Baseledger: a public-permissioned, council-governed network that fulfills the major requirements of enterprise organizations for participating in baseline-enabled processes.

We propose an Architecture of Architectures, introducing Baseledger as the underlying ledger for coordinating leaf node consensus, configuration, public DID registries and protocol interoperability enabling workflow exits and tokenization ("Layer 1") and privacy-preserving workflow and workstep rollups under zero-knowledge ("Layer 2"). Baseledger is a novel proposal in that no existing projects have aimed to coordinate Layer 1 and Layer 2 within a single, open architecture.

Baseledger itself can serve as the minimum viable protocol to serve Layer 2 functionalities and exit them into Layer 1 by storing baselined proofs in the network. Additionally, Baseledger always works as the underlying Ledger for coordinating any multi-chain setups, e.g., combining Baseledger with Ethereum for DeFi.

Baseledger equips enterprise ecosystems (i.e, groups of entities leveraging public blockchain as a state machine in tandem with a consensus mechanism facilitating the enablement of zero-knowledge privacy protocols) with best-of-breed infrastructure for adopting the Baseline protocol using pluggable Layer 1 and Layer 2 consensus mechanisms. The infrastructure abstracts the network, registry, key management, messaging and privacy components of the protocol from the context of Layer 1 and Layer 2.

This enables enterprise applications to leverage this powerful protocol for advanced business process automation. Baseledger is industry-agnostic and supported consensus configurations will always enable scalable off-chain transaction throughput on Layer 2 and Enterprise DeFi on Layer 1.

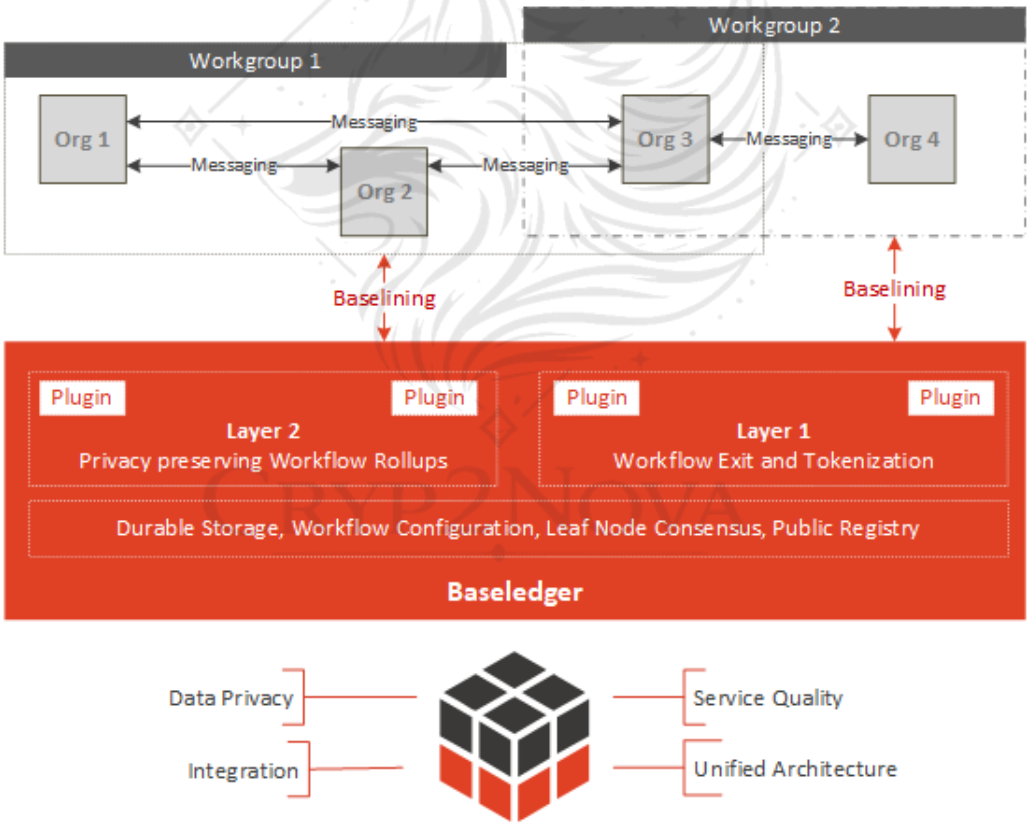
Archived copy · cryp2nova.com

4.1 Architecture of Architectures

Baseledger can be thought of as an *architecture of architectures* in the context of supporting pluggable, interoperable consensus across Layer 1 and Layer 2 (together, a "*Protocol Pair*"). The proper notation for defining a Protocol Pair is as a tuple, i.e.:

(LAYER 1 PROTOCOL, LAYER 2 PROTOCOL)

- where Layer 1 represents the layer for storing final states, for a notarized "exit" of a business process (an exit can be the storing of a final proof and/or the conversion into a token)
- where Layer 2 represents the layer for representing distributed business workflows and zero-knowledge proofs to be rolled up into Layer 1



Each peer, in this context, retains full independence from the network consensus mechanism which is used to create crypto economic incentives related to network security, privacy, quality of service and governance. A network peer (or *Node*) can be containerized, run on bare metal, or public cloud infrastructure, etc. An organization which runs a Node is referred to as an *Operator*.

Archived copy · cryp2nova.com

The required (and optional) software interfaces are provided by the core Baseline Protocol packages. The infrastructure interfaces provided by this specification underscore how a collection of microservice, messaging and peer-to-peer client components, when viewed as a single homogenous appliance, comprise a Baseline-compliant *full node* representing a single network peer. Alternatively, a *leaf node* is a light client node — that anyone can run from anywhere — and provide redundancy around peering and configurations for the network.

The Baseledger network *consensus* mechanism underlying any Protocol Pair is Tendermint consensus. This *consensus* ensures each *operator* running a Baseledger *full* or *leaf* node remains synchronized with the rest of the ecosystem.

With this architecture, Baseledger can run autonomously and/or coordinate other Multi-Chain setups with Protocol Pairs, being candidates for reference support upon the launch of the Baseledger mainnet. Examples are presented in Chapter 5.

CRYP2NOVA

Archived copy · cryp2nova.com

4.2 Consensus Model

4.2.1 Tendermint Introduction

Within the Baseledger implementation, we use and fork Tendermint[23]. Tendermint BFT is a solution that packages the networking and consensus layers of a blockchain into a generic engine, allowing developers to focus on application development as opposed to the complex underlying protocol. Tendermint Core is a blockchain application platform; it provides the equivalent of a web-server, database, and supporting libraries for blockchain applications written in any programming language. Like a web-server serving web applications, Tendermint serves blockchain applications. More formally, Tendermint Core performs Byzantine Fault Tolerant (BFT) State Machine Replication (SMR) for arbitrary deterministic, finite state machines.

The Tendermint BFT engine is connected to the application by a socket protocol called the Application Blockchain Interface (ABCI). This protocol can be wrapped in any programming language, making it possible for developers to choose a language that fits their needs.

Many novel blockchains rely on BFT, including Cosmos.Network on Tendermint, and Libra on LibraBFT (built upon HotStuff). The Tendermint open-source project was born in 2014 to address the speed, scalability, and environmental issues of Bitcoin's proof-of-work consensus algorithm by using and improving upon proven BFT algorithms developed at MIT in 1988[24].

Tendermint is a partially synchronous BFT consensus protocol derived from the "DLS consensus algorithm"[25]. Tendermint is notable for its simplicity, performance, and fork-accountability. The protocol requires a fixed known set of validators, where each validator is identified by their public key. Validators attempt to come to consensus on one block at a time, where a block is a list of transactions. Voting for consensus on a block proceeds in rounds. Each round has a round-leader, or proposer, who proposes a block. The validators then vote, in stages, on whether to accept the proposed block or move on to the next round. The proposer for a round is chosen deterministically from

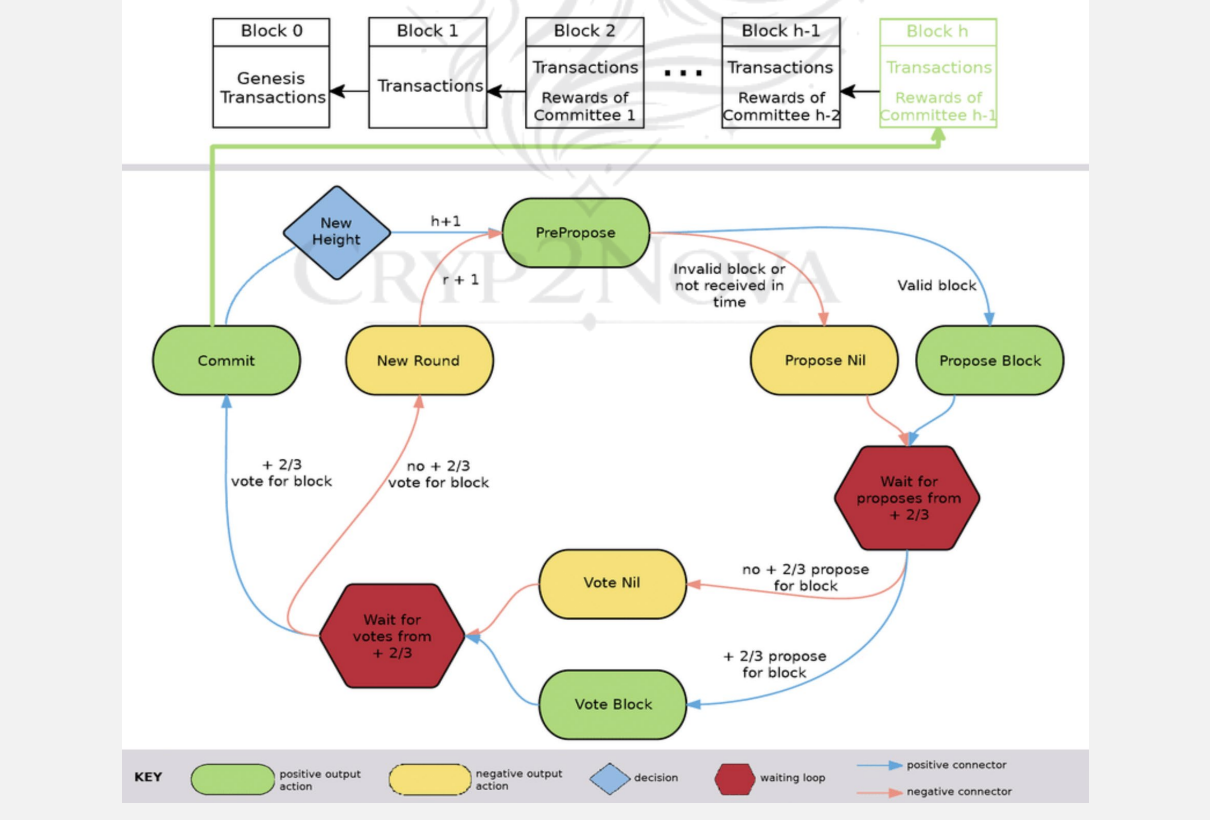
[23] https://tendermint.com/static/docs/tendermint.pdf
[24] https://groups.csail.mit.edu/tds/papers/Lynch/jacm88.pdf, Consensus in the Presence of Partial Synchrony, CYNTHIA DWORK, NANCY LYNCH, LARRY STOCKMEYER, IBM Almaden Research Center, San Jose, California
[25] https://cosmos.network/resources/whitepaper

Archived copy · cryp2nova.com

the ordered list of validators, in proportion to their voting power. The full details of the protocol are described in the Tendermint Github[26]. Tendermint's security derives from its use of optimal Byzantine fault-tolerance via super-majority (>⅔) voting and a locking mechanism. Together, they ensure that:

- ≥⅓ voting power must be Byzantine to cause a violation of safety, where more than two values are committed.
- If any set of validators ever succeeds in violating safety, or even attempts to do so, they can be identified by the protocol. This includes both voting for conflicting blocks and broadcasting unjustified votes.

In classical Byzantine fault-tolerant (BFT) algorithms, each node has the same weight. **In Tendermint, nodes have a non-negative amount of voting power, and nodes that have positive voting power are called validators**. Validators participate in the consensus protocol by broadcasting cryptographic signatures, or votes, to agree upon the next block. The following diagram shows[27] the way Tendermint works in terms of voting, consensus finding and block generation.

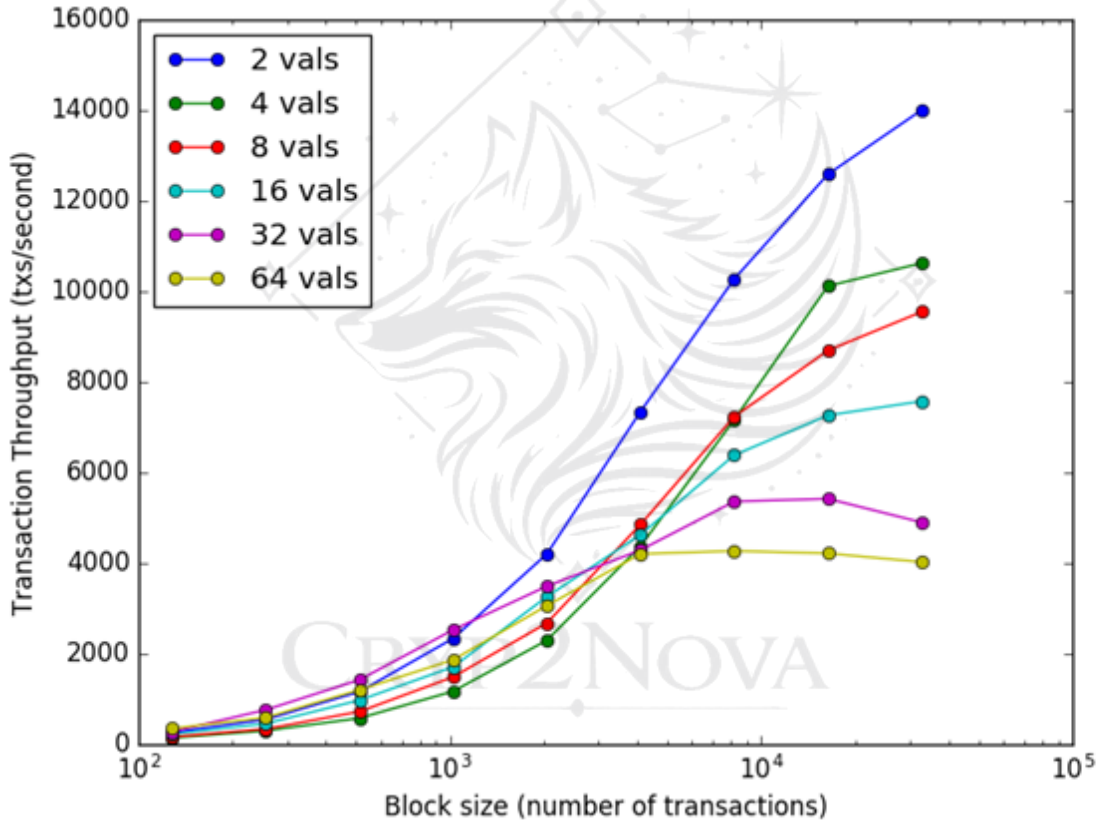


[26] https://github.com/tendermint/tendermint
[27] taken from: http://atrium.lib.uoguelph.ca/xmlui/bitstream/handle/10214/9769/Buchman_Ethan_201606_MAsc.pdf

Archived copy · cryp2nova.com

4.2.2 Performance Considerations

Tendermint BFT can have a block time on the order of 1 second and **handle up to thousands of transactions per second**. In benchmarks of 64 nodes distributed across 7 data centers on 5 continents, on commodity cloud instances, Tendermint consensus can process thousands of transactions per second, with commit latencies on the order of one to two seconds. Notably, performance of well over a thousand transactions per second is maintained even in harsh adversarial conditions, with validators crashing or broadcasting maliciously crafted votes. See the figure below for details[28].



A property of the Tendermint consensus algorithm is instant finality. This means that forks are never created as long as more than a third of the validators are honest (Byzantine). Users can be sure their transactions are finalized as soon as a block is created (which is not the case in Proof-of-Work blockchains like Bitcoin and Ethereum).

Tendermint consensus is not only fault tolerant, it is also accountable. If the blockchain forks, there is a way to determine liability.

[28] taken from: http://atrium.lib.uoguelph.ca/xmlui/bitstream/handle/10214/9769/Buchman_Ethan_201606_MAsc.pdf

Archived copy · cryp2nova.com

4.3 Token Model

As part of the Solution, we propose an extension of the existing UBT token to serve as a hybrid working and payment utility token for Baseledger.

4.3.1 Context on Utility Tokens

There is broad agreement on distinguishing three types of tokens: **stores of value, security tokens, and utility tokens**. Within the Baseledger definition, we focus on utility tokens[29] and propose the following distinction - in our technical understanding - for utility tokens: **payment tokens and work tokens.**

Payment (utility) tokens

The majority of ICOs[30] that launched in recent years involved utility tokens that also acted as proprietary payment tokens, for example Filecoin, 0x, or BAT (Basic Attention Token). Each of these cryptocurrencies presents itself as an independent monetary base. The overall idea is that such an asset serves as the exclusive form of payment that the network will accept in exchange for an underlying scarce resource that it provides (bandwidth, storage, computation, and so forth).

As argued by Kyle Samani[31], most of these proprietary payment currencies are, generally speaking, susceptible to the **velocity problem**, which might exert perpetual downwards price pressure. This is because many of these projects are thought to be at risk of having their token price decoupled from network value.

$$Network\ Value\ (marketcap) = \frac{Transaction\ Volume}{Velocity}$$

Network value is the monetary value of the entire token ecosystem (i.e. monetary base). Transaction volume, on the other hand, represents the actual utility that users get from using the network. At the heart of this serious issue, called by many as the "velocity thesis," is the gradual decoupling of the token's utility value (e.g. to purchase

[29] We will leave aside security tokens as they are irrelevant to this discussion – having securities on a blockchain does not change anything about the legal or regulatory nature of the security.
[30] Initial Coin Offerings
[31] https://multicoin.capital/2017/12/08/understanding-token-velocity/

Archived copy · cryp2nova.com

bread) from network value. The thesis predicts the final result with a decrease of the token value and an eventual network collapse.

The overall argument is that tokens that are not store-of-value assets will generally suffer from high velocity at scale as users avoid holding the asset for meaningful periods of time, suppressing ultimate value. In a world where these platforms are mature and integrated into our daily lives, there would be hundreds and thousands of coins for everyone to manage. Most likely, people wouldn't store the various coins they use. Rather, they would hold one or more general purpose currencies. That way they would have flexibility on when and which coins they use, without having to worry about the price fluctuations[32].

Obviously, payment tokens focus on the demand side (customers paying) rather than on the supply side (product and service work offered).

As a token model, payment tokens do not fit all applications as they most often introduce complexities for the platform that need to be handled. These models are thought to work, for example, when addressing very specific niches or customers segments, when those customers can bear to handle and hold the respective payment token and want to reserve a certain share of the product or service the token allows for.

A successful example of a payment utility token model might be the current usage of the Unibright UBT Token, that follows the idea of a payment token by acting as a voucher to access Unibright's Product and Services: As these services are limited (scarce) and aim at a specific group of users (enterprise customers) this model works with enterprise customers reserving their needed share of Unibright's products and services by holding UBT and locking it, for example, within the Unibright Framework or putting it into custody. As UBT is understood to be an "initial access token", whose balance can be refilled monthly by FIAT[33] payments, it also mitigates the velocity problem towards enterprise usage. Additionally, a good payment token model has to be updated and adopted to the (changing) environments and customer's needs — that is why Unibright's token model for example is evaluated and updated periodically.

[32] https://hackernoon.com/token-velocity-a455173d69e3
[33] Fiat money is currency that is not backed by a physical commodity, such as gold or silver, but rather by the entity that issued it. The value of fiat money is derived from the relationship between supply and demand.

Archived copy · cryp2nova.com

Work (utility) token

Within the work token model, a service provider stakes the native token of the network to earn the right to perform work for the network. For services which have to be commodity-like such as Keep (off-chain private computation), Filecoin (distributed file storage), Livepeer (distributed video encoding), Truebit (off-chain verifiable computation), the probability that a given service provider is awarded the next job is proportional to the number of tokens staked as a fraction of total tokens staked by all service providers. Kyle Samani offered a great introduction on the term "work token" in the realm of general utility tokens in "New Models for Utility Tokens"[34].

One attribute of the work token model is that, absent any speculators, increased usage of the network can cause an increase in the price of the token. As demand for the service grows, more revenue will flow to service providers. Given a fixed supply of tokens, service providers may rationally pay more per token for the right to earn part of a growing cash flow stream.

Most work tokens systems enforce some sort of mechanism to penalize workers who fail to perform their job to some pre-specified standard. For example, in Filecoin, service providers contractually commit to storing some data for a period of time.

Payment Token vs. Work Token

While both token types — payment token & work token — can still be considered utility tokens, they differ significantly. The most apparent difference is that payment tokens function as electronic money that is used to buy a resource. Work tokens, on the other hand, provide the right (via staking) to perform work in the network.

Distinctions can be pointed out across three important categories:

- **Consensus Mechanism**: The payment token (regardless of the underlying consensus) uses a one-to-one injective function and does not need special consideration regarding its incentive structure. On the other hand, the work token requires thoughtful implementation of a Proof-of-Stake (PoS) consensus mechanism that ensures all interests are properly aligned.

[34] https://multicoin.capital/2018/02/13/new-models-utility-tokens/

Archived copy · cryp2nova.com

■ **Function of Money**: The payment token is used as a medium-of-exchange to facilitate payment from the consumer to some resource provider. On the other hand, the work token functions as a specific unit-of-account that is used to reserve the right (via staking) to do work beneficial to the network.

■ **Layer Touch Point**: The payment token is visible throughout the application-level to both: resource provider and consumer. On the other hand, the work token is completely abstracted from view and is instead handled by a whole new set of actors that interact in the layers below the level of the application.

These kinds of work tokens — aside from the technical differences — present three very useful innovations for any protocol that chooses to use them:

1. They help with network security by deterring any potential attack via a slashing function.
2. They help with network quality by attracting participants who work to improve the network's product or service proposition.
3. They force the valuation model to change from equation-of-exchange to net-present-value.

The last point simply means that network value becomes better aligned with token value. Specifically, as network usage grows, so does token value in a (super)-linear fashion.

From an economics perspective, it is important to point out that a work token is vital to the supply side of the market (service/product offering), whereas a payment token is vital to the demand side of the market (customers using it to pay). This potential distinction leads to a benefit for (enterprise) customers using the network – they do not necessarily need to handle the native token of a project – payment can be made using any (crypto)currency.

A look at supply and demand in the market a token serves can help to distinguish between payment and work utility tokens: **If the demand side (customer side) is the primary aim for optimizing the token model, a payment token might fit. If an incentivized ecosystem is the main target (supply side), a work token might come into mind.**

Archived copy · cryp2nova.com

4.3.2 Requirements for the Baseledger Token Model

The core feature of tokenized ecosystems (public blockchains) **is encouraging participants to do work**. Incentives are powerful — as well described by Charlie Munger: "*Show me the incentive and I will show you the outcome.*" Blockchains can be seen as incentive machines: one can get participants to do work by rewarding them with tokens. To be more specific, the (block) reward function defines what networks do.

In many examples of the former presented token models, there is one misalignment in terms of incentives: a token ecosystem most often will have token holders that cannot, or do not, want to do work within the ecosystem (i.e. stake but no work). On the other hand, there are possible workers with the resources to work but not the tokens to stake (i.e. work but no stake).

This leads to situations where there is no real incentive for a community to initially fund or build an ecosystem, and later engage in running the product (by doing work). This is a problem well-known from classic business models: revenue most often comes later or is too small – funding is needed while building the product and ecosystem.

Considering the fact that Baseledger serves a B2B functionality, it is important to define the requirements of the token model:

a) The ecosystem is comprised of the individuals who hold tokens but do not necessarily use them or have the resources to do "work";
b) The workers are resource owners that do the work, but do not necessarily own tokens or use the service itself;
c) The users are organizations that actually use the service but are not necessarily interested/allowed to buy or hold cryptocurrency

The token model should enable token holders to "rent out" their stake to resource owners, resource owners to do "work" (without being token holders themselves), and users to use Baseledger without being token holders.

It is still absolutely possible that a Baseledger user is a token holder, worker, and user at the same time, but this should not be mandatory in a B2B environment.

Archived copy · cryp2nova.com

Thus, we define the major requirements for the Baseledger token model:

1) Incentivize the ecosystem to own and hold tokens to drive Baseledger
2) Incentivize the workers to provide the working resources for keeping Baseledger up and running
3) Incentivize the users to use the services without the compulsory obligation to be part of the ecosystem or workers

4.3.3 Extension of the Existing UBT Token Model

There are two ways to create the Baseledger token described above:

1) By creating a new token (e.g., by doing an IEO (Initial Exchange Offering) and building the needed token ecosystem)
2) By incorporating Baseledger tokenomics into the existing Unibright Token (UBT).

Both scenarios were strongly considered. Although it may have been easy to run a successful IEO based on Baseledger and its optimistic outlook, we decided to leverage the existing Unibright ecosystem, since the UBT token is well-established in the blockchain-business integration vertical and also widely distributed.

There is already a set of products and services powered by the UBT token[35] within Unibright's and Provide's product offerings. Nevertheless, we believe Baseledger is a perfect extension to these offerings. By combining them, UBT is not only an "input" payment token, but also an "output" reward token, which makes the token flow complete.

[35] https://unibright.io/#token

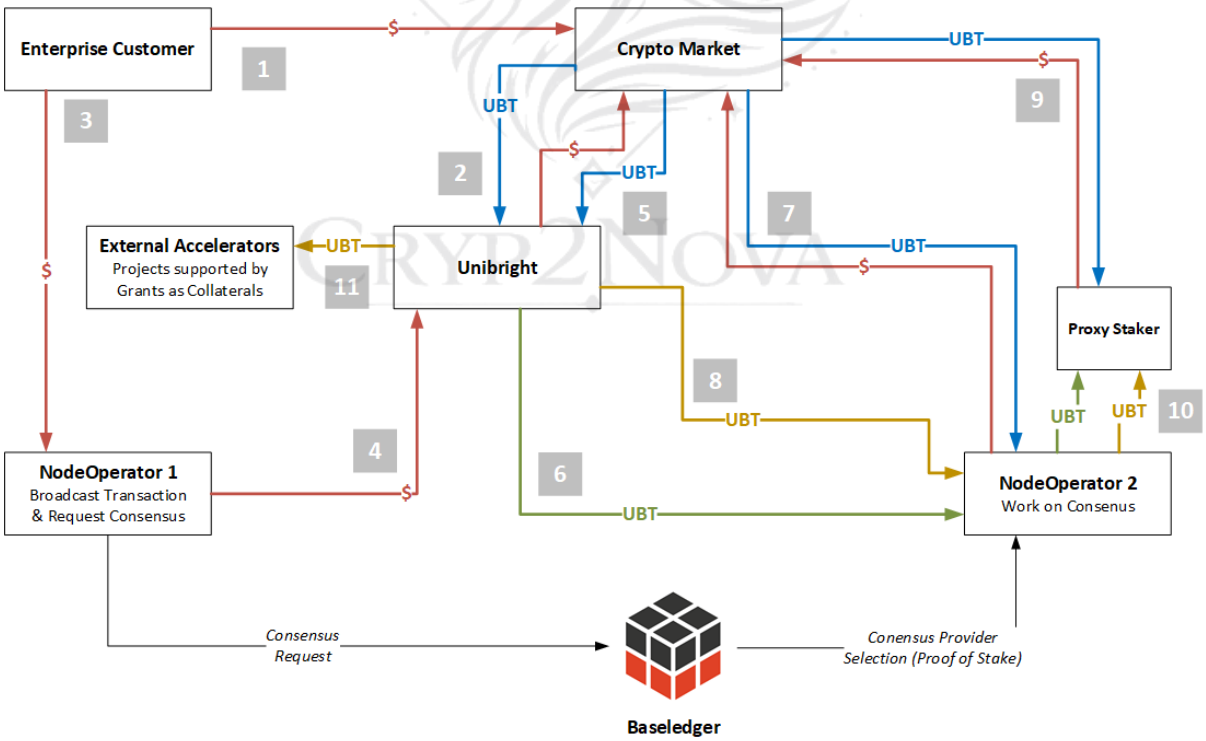
Archived copy · cryp2nova.com

4.3.4 The Baseledger Token Model

We propose a utility token model where:

- The token acts as a payment mechanism for using software
- The token acts as a staking mechanism for workers maintaining consensus
- The token acts as a "share-in-the-block reward" mechanism for workers that are doing the work
- A proxy-staking mechanism is in place, where members of the ecosystem can contribute to a worker's stake (and partially participate in the rewards) without doing the work themselves
- Organizations (users) do not need to handle the token themselves and can pay in fiat money

The following diagram shows the token and fiat streams envisioned in the tokenized ecosystem of Baseledger, incorporating aforementioned elements like revenues, rewards and customer payments.



Archived copy · cryp2nova.com

Current Model

Items 1 and 2 show the current model, establishing UBT as the "Universal Business Token", the voucher to use blockchain integration services:

1) An enterprise customer wants to use software[36] from Provide and Unibright. To start a contract, an initial payment of UBT is needed. The customer can buy these tokens directly on the open market or with the help of Payment services[37].
2) These UBT tokens are stored safely by Unibright in external custody[38]. A portion (up to 50%) of these UBT can be used to cover native blockchain transaction costs, like gas in Ethereum (="*integration cost portion*").

Extension for Long-Term Sustainability

Items 3-6 show the Baseledger related token model extension to promote long-term sustainability by taking a fee from the transactions and redirecting it to the ecosystem:

3) A *Node Operator 1* with the task to broadcast Baseline conformant messages and to request consensus is paid for his services in Fiat. These Node Operators can be run by parties[39] who sign an SLA[40] with the Baseledger Council.
4) A part of these fiat payments is shared with Unibright.
5) Unibright uses this fiat payment to buy UBT from the open market[41]…
6) ...and use it as a revenue share with the *NodeOperator 2*

CRYP2NOVA

[36] For example, the Provide Framework (formerly Unibright Framework), the Unibright Connector, Provide Shuttle, Ident or NChain

[37] For example, Provide Payments exposes a Managed Transactions API which calculates the amount of UBT needed to cover the underlying blockchain transaction costs (i.e., gas) at runtime, based on the current exchange rate of UBT against the native cryptocurrency of the target network (i.e. ETH). A hot wallet managed by a professional custodian service is used to fund transactions which are broadcast by Provide on behalf of customers using the API. Customers are billed in arrears on the first of each month for their usage during the previous month.

[38] Professional custody providers, for example Coinbase Custody

[39] For example, Provide, Unibright, other organizations or third parties

[40] Service Level Agreement

[41] For example, through Provide Payments

Archived copy · cryp2nova.com

Extensions for an incentivized ecosystem

Items 7-11 support short-term growth and an incentivized ecosystem independent from network revenue. They create a complete ecosystem around both the tools and services to baseline business processes and Baseledger itself.

7) For a *NodeOperator2* to be selected as a consensus worker through Proof-of-Stake, UBT have to be bought from the open market to build the stake
8) As less integration costs for other protocols are needed, NodeOperators can be additionally rewarded from the integration cost portion, especially in the bootstrapping phase, where the revenue share from 6 may not cover all costs of providing a full node.
9) Proxy stakers, who are not able to perform the work of a NodeOperator can (by private contracts with Node Operators and/or an envisioned smart contract based decentralized solution) delegate their stake to an existing node operator and...
10) … participate in revenue shares and rewards (potentially according to a smart contract that handles staking, rewards and potential fines related to the node operator contract)
11) Additionally, UBT from the integration cost portion can be used to incentivize individuals, teams, or companies adding to the overall potential of the Baseledger ecosystem, for example by building adjacent products, services, or add-ons.

CRYP2NOVA

Summary

The planned model has the potential to successfully support the distinction between and proper addressing of both the *enterprise audience* (interested in Software-as-a-Service with a classic fiat payment model) and the *cryptocurrency audience* (interested in holding and staking UBT and participating in revenues and rewards).

Tokens that have been used for customer projects earlier in 2019 and 2020 remain stored safely by Unibright in external custody. Revenue shares and rewards can be covered by tokens coming from new enterprise customers in 2021 and later.

Archived copy · cryp2nova.com

This would create a framework for a self-sustaining ecosystem that is able to grow and incentivize those working on it. It is vital to understand that the curating/governing is done in a way whereby funds are given to those that add to the network's overall revenue and growth. As described, two main paths to reward workers are shown: The first is a network reward paid to those maintaining the Baseledger nodes; the second is giving grants to entities that work on the product and ecosystem in a meaningful way.

The complete vision is a token model that helps to grow the network around Baseledger. The more network usage occurs, the more tokens get staked, leading to higher demand. Additionally, more usage should lead to more revenue which is partly returned to the network to incentivize workers.



Archived copy · cryp2nova.com

4.4 Council and Governance

Baseledger will be governed by the Baseledger Council which consists of recognized companies and individuals from the Enterprise Blockchain space and adjacent sectors. In the beginning, the council is expected to have 5-9 members including the founding companies. The Baseledger Council is set to grow constantly with an ever-broader set of parties to be included. A written contract signed by all council members guarantees their consent on the overall rules and conditions — ensuring they work for the long-term benefit of the Baseledger Network.

The primary and foremost task for the council members is to actively work on the governance of Baseledger. This includes running nodes themselves and appointing parties to run nodes with respect to the governing rules for the network. The council members will work on adjusting the overall rules and conditions of the network if necessary, work jointly on the core-software (along with the public source community), manage network pricing, drive customer onboarding, and work on a flexible path to make sure that compliance with legal regulations is reached.

The council members will vote on all matters and will have a scheduled fixed set of meetings in various working groups with appointed chairs. The overall goal is for Baseledger to be the leading enterprise-grade DLT solution. The long-term interest of Baseledger is the agreed-upon maxim for the council — a goal that is mandatory to be shared by all council members.

CRYP2NOVA

Archived copy · cryp2nova.com



Archived copy · cryp2nova.com

5 Reference Implementation Examples

5.1 Phases and Process Flow of an Example Use-Case

We now consider an example use case of a procurement process, with the potential to exit into a tokenized invoice.

In the **initialization phase**, participants of the business process set up organization registries, workgroup shields and workflow verifiers, according to the Baseline Protocol.

In the **phase of (repeated) worksteps**, the participants baseline their business process. The document flow starts with purchase orders, and continues with order confirmations, shipping notifications, goods receipts and subsequently invoices.

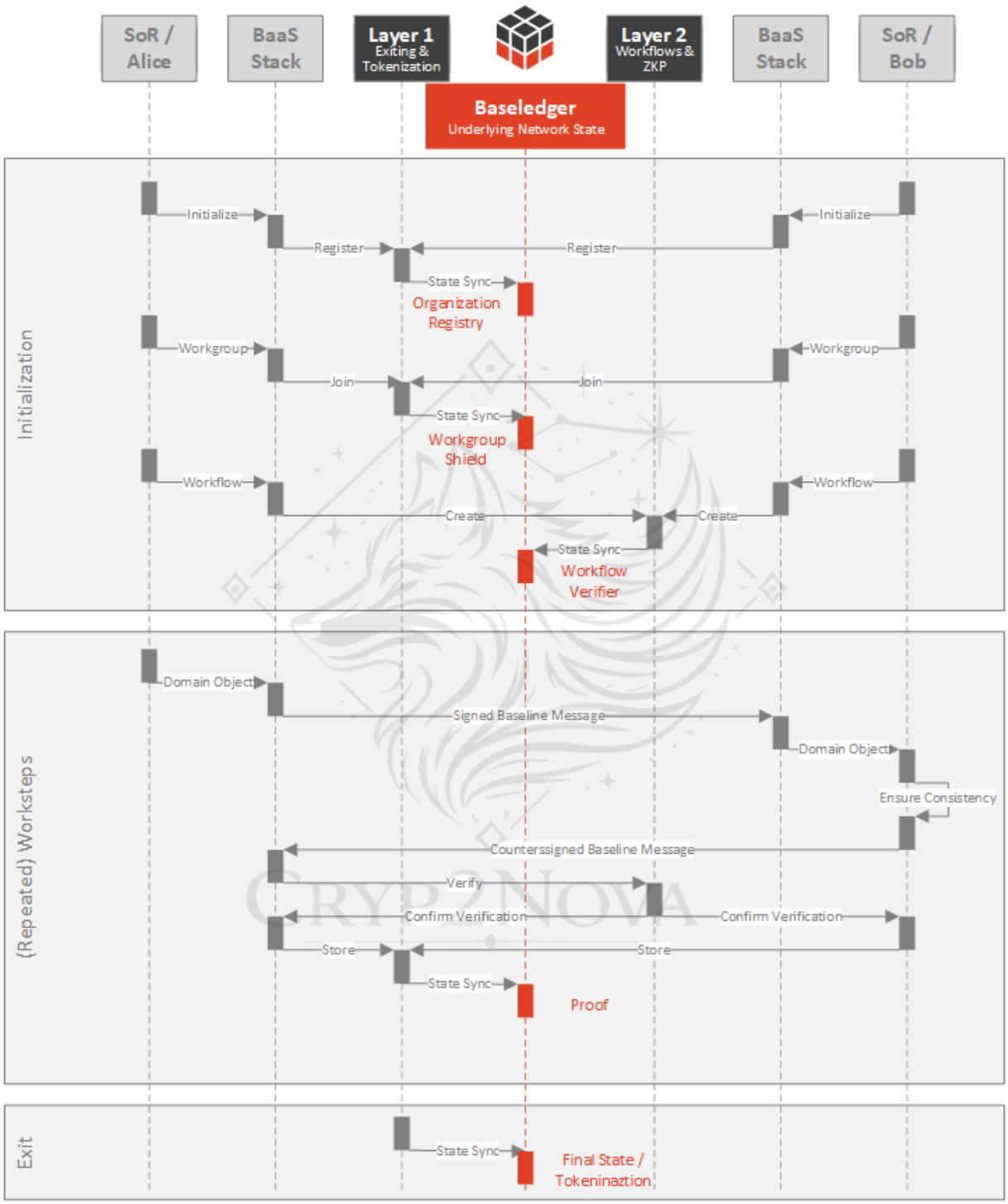
These documents, coming from one participant's System of Record (*SoR*, for example an SAP ERP) are transformed into a common domain model that all participants are able to read and write to, and then sent to suppliers over secure channels, according to the patterns of the Baseline Protocol.

Changes to the purchase order, e.g., due to quantity adjustments or material substitutes, are exchanged between the buyer and supplier to keep their respective systems of record in sync.

Proofs of state synchronization are notarized on Baseledger, the Mainnet, without revealing the sensitive content of the business data to third parties. In reference implementations, this happens automatically between different Provide and Unibright *Baseline-as-a-Service* stacks, a Protocol Pair Tuple and Baseledger itself.

In the **exit phase**, proof of the final state is notarized, and can be used as a trigger for tokenization to enable automated payment or **Enterprise DeFi** ("Decentralized Finance") applications.

Archived copy · cryp2nova.com

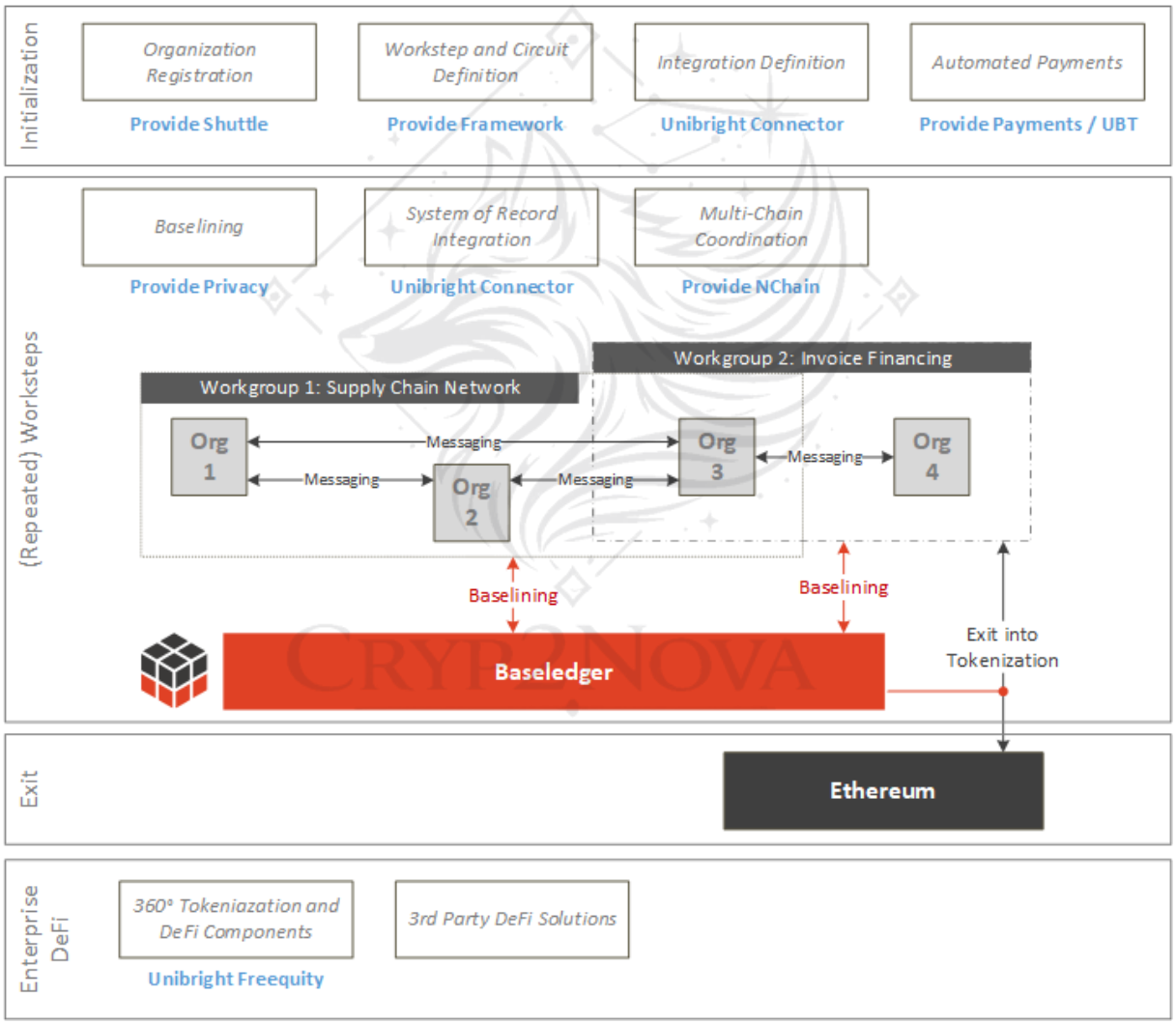


Archived copy · cryp2nova.com

5.2 Example Setups

The following examples show the different alternatives in which Baseledger can be operated: Baseledger can serve as the basic protocol to serve Layer 2 functionalities and act as Layer 1 by storing baselined proofs in the Baseledger network. Additionally, Baseledger always works as the underlying Ledger for coordinating any multi-chain setups, e.g., combining Baseledger with Ethereum for DeFi.

In all setups, different components from the combined Provide-/Unibright tech-stack[42] are used in all phases as described in chapter 5.1



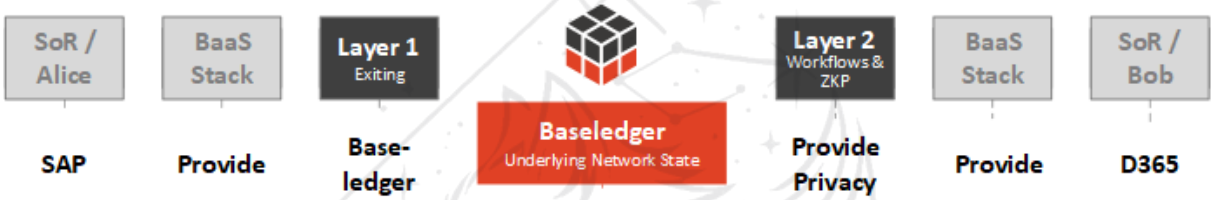
[42] See provide.services

Archived copy · cryp2nova.com

5.2.1 Example 1 - Pure State Synchronization

Two enterprise organizations want to synchronize business processes, and by extension their off-chain systems (SAP, Microsoft Dynamics or Excel), without post-exit asset tokenization. In this case, workflows and worksteps are handled and verified by a solution on every Baseline-as-a-Service stack (e.g., Provide Privacy).

The intermediate, entangled workstep proofs are stored within Provide Privacy; the workflow exit proof is stored in Provide Privacy (i.e., for future counterparty verification of this individual exit or this exit in the context of an arbitrarily-sized rollup commitment) and on Baseledger itself:



5.2.2 Example 2 – Post-Exit Tokenization

Two enterprise organizations want to synchronize business processes, and by extension their off-chain systems (SAP, Microsoft Dynamics or Excel). One or both seeks post-exit asset tokenization (e.g., factoring or financing the invoice payment). In this case, workflows and worksteps are handled and verified by a solution on every Baseline-as-a-Service stack (e.g., Provide Privacy).

The intermediate, entangled workstep proofs are stored within Provide Privacy; the workflow exit proof is stored in Provide Privacy (i.e., for future counterparty verification of this individual exit or this exit in the context of an arbitrarily-sized rollup commitment) and on the public Ethereum mainnet itself (i.e., ideal for when this exit proof is associated with one or more tokenized financial instruments).

Archived copy · cryp2nova.com

In this case, Baseledger provides durable storage and fault-tolerance for workgroup and workflow configurations, coordinates leaf node consensus across a global mesh network of low-latency baseline operators and replicates public registries (e.g., organizations and DIDs):



5.2.3. Example 3 - Orchestration of other Protocols

As a future-proof solution, Baseledger can orchestrate other solutions for Layer 1 and Layer 2 that may be needed in specific environments or may include future protocols with different feature sets. In these cases, the Baseledger standards for integrating off-chain systems AND for state synchronization remain untouched, so that Enterprise customers do not have to worry about underlying, protocol-specific implementation details. The Protocol Pair, serving for Layer 1 and Layer 2 functionalities, can be plugged-in or exchanged when needed.



Archived copy · cryp2nova.com

5.3 Solution Details

5.3.1 Service Quality

Performance

The solution to performance-related problems comes from the consensus algorithm provided by Tendermint (on which Baseledger is built). Tendermint, an algorithm for reaching consensus among known validator nodes, utilizes Byzantine Fault Tolerance, which means that it avoids limitations from which regular PoW/PoS consensus algorithms suffer performance-wise. From the Cosmos Network[43] whitepaper[44]:

"Despite its strong guarantees, Tendermint provides exceptional performance. In benchmarks of 64 nodes distributed across 7 datacenters on 5 continents, on commodity cloud instances, Tendermint consensus can process thousands of transactions per second, with commit latencies on the order of one to two seconds. Notably, performance of well over a thousand transactions per second is maintained even in harsh adversarial conditions, with validators crashing or broadcasting maliciously crafted votes."

The performance of Baseledger comes from two facts. Firstly, the validator nodes in the network are known, so there is no need to have additional algorithm checks in place to make sure that the behavior is not malicious. Validators can join the network based on a predefined process which is defined outside of the technical implementation, and are accountable for their actions on the network. In the case of Baseledger, it is the job of the governing body to set up a process through which an entity can become a validator, and through which that entity commits to a legal framework that ensures accountability and security of the network. Additionally, Baseledger utilizes proof of stake on top of the Tendermint BFT algorithm, further increasing the security of the network by having an option to financially penalize malicious behavior of validator nodes.

[43] The Cosmos Network is a decentralized network of independent, scalable, and interoperable blockchains, creating the foundation for a new token economy. It is built on top of Tendermint.
[44] https://cosmos.network/resources/whitepaper

Archived copy · cryp2nova.com

Secondly, since the validators are known, the network does not need a large number of validators to keep it safe, as is the case with public blockchain. For example, the Cosmos Network launched with a maximum of 100 validator nodes with plans to increase this number to not more than 300 in the next 10 years[45].This means that state can be quickly propagated through the network without fear of chain forks, further improving throughput while enabling transaction finality times on the order of one or two seconds[46].

The Baseledger consensus algorithm solves in multiple ways another problem related to performance: performance predictability or the Noisy Neighbor problem. Firstly, the Tendermint BFT proof of stake algorithm greatly increases throughput thus increasing the level of activity needed to affect the performance of the network. Secondly, since every participant's identity is known, malicious behavior is discouraged. Thirdly, the governing body ensures SLAs related to uptime and performance are fulfilled, because operators (nodes) are legally bound to these agreements.

Transaction Costs

The unpredictability of transaction costs is another problem with the utilization of public blockchains in enterprise applications. This derives from the fact that transaction fees are used to allocate the resources of traditional blockchain networks (i.e., the computing power of miners) across users' transactions, while protecting against DOS attacks by imposing an economical barrier. Miners, by nature of performing the work, can choose which transactions they want to include in a block. As a result, users choose to pay higher miner rewards (in the form of gas costs) per transaction, so that their transactions are prioritized. This creates a feedback loop whereby, in periods of higher network activity, gas costs grow dramatically and unpredictably.

Baseledger's solution to this derives from the fact that the validators of the network are known and held accountable. This means that the transaction cost does not have to serve the role of protecting the network against DOS attacks. Also, since Baseledger uses proof of stake consensus, validators do not have to utilize expensive computing resources to create new blocks.

[45] https://blog.cosmos.network/economics-of-proof-of-stake-bridging-the-economic-system-of-old-into-the-new-age-of-blockchains-3f17824e91db

[46] Same as 13

Archived copy · cryp2nova.com

This in turn allows Baseledger's governing body to set transaction fees for fixed periods of time and use these fees for work other than transaction validation. Validators are periodically rewarded based on the number of transactions validated and any remaining fees can be distributed among projects who are working to improve the protocol, thus increasing the value of the whole network.

5.3.2 Data Privacy

To ensure **Data Mutability**, Baseledger proposes an elegant solution using encryption keys: all transaction data received by a Baseledger node is encrypted symmetrically and the corresponding key is stored safely off-chain by each node. If necessary, for example in the case of a regulatory investigation, nodes are able to decrypt the data by retrieving the key.

This setup enables data owners to at any point "delete" sensitive data by requesting nodes to delete the encryption key. This maintains the integrity of the chain while fulfilling data privacy rights. The process of deleting encryption keys will be audited and involve a Proof-Of-Deletion receipt, so that it is demonstrable. In other words, by deleting the keys that were used to encrypt data, the data can no longer be accessed by any participant even though encrypted copies remain on Baseledger nodes.

Additionally, this mechanism can be used to satisfy the right of **rectification** in a compliant manner: by "deleting" data as described and adding updated data to the network in a new transaction.

To ensure compliance in terms of **Data Residency**, only computing units in jurisdictions that comply with the agreed-upon privacy rules will be granted membership and the ability to operate a node.

To fulfill the needs of **Data Democracy**, we suggest a council-governed public blockchain. We propose a public blockchain, whose node operators are known and bound to data processing and data storage agreements. This empowers those who

Archived copy · cryp2nova.com

are generating data to control it, by granting them the rights to delete, modify, transfer and govern their data as described above.

For enterprise applications, these features are a necessity. Within Baseledger, data compliance and democracy are included by design.

5.3.3 Integration

Technical Business Integration

In the past decades, several technical approaches to business integration have been established. In our understanding, Blockchain technology should be seen as an extension to existing middleware or cloud-based architectures, which have already replaced outdated point-to-point architectures[47].

Blockchain has clear advantages in various areas of business integration. Still, it will most probably be just one part of a complete business integration architecture, working alongside existing IT landscapes. From this, a conclusion can be drawn: to benefit from the promises the blockchain offers, we need a holistic solution that allows us to integrate specific blockchain technologies into existing IT- and business integration landscapes.

Unibright developed the Unibright Framework to integrate blockchain technology into existing off-chain ecosystems with a focus on enterprise integration. The Unibright Framework is now the *Provide Framework* (part of Provide[48]) and is an embedded component in Provide's vertically-integrated Baseline-as-a-Service offering: Shuttle. Shuttle enables no-code workgroup and environment configuration for each organization in an ecosystem, automated container orchestration supporting Kubernetes or Provide's container runtime on customer-owned infrastructure (e.g., AWS, Azure) and orchestration of these resources in the context of the Baseline Protocol.

[47] D. Yuri, C. Ngo, R. Strijkers, and C. De Laat, Defining inter-cloud architecture for interoperability and integration, CLOUD COMPUTING, 2012.
[48] https://provide.services/technology/framework

Archived copy · cryp2nova.com

The Provide Framework streamlines the effort coming out of traditional enterprise consulting services, in collaboration with a customer's business process and domain knowledge. Visually-designed domain models are then transformed into code-generated artifacts such as smart contracts, oracles, and zero-knowledge circuits. With code-generated APIs and proxies, instances of these domain models are orchestrated in the context of an organization's ERP system and other off-chain systems of record.

The Provide stack serves as a protocol- and cloud-agnostic reference implementation for the Baseline Protocol and this same flexibility makes it well-suited to play a significant role within the first reference implementation of Baseledger. The alliance formed by Unibright and Provide enables sustainable, domain model-oriented integration of off-chain systems with advanced messaging, privacy and web3 technologies generally. The UBT token model seamlessly serves dual roles as the *Universal Business Token* and native currency on the Baseledger mainnet.

Blockchain Specific Integration Tasks

The presented extension of the UBT token model enables a clear value proposition for both the enterprise user and blockchain audience. The utility of the token is extended without affecting the performance of the solution itself. Furthermore, services like Provide Payments ensure that actual market interaction with tokens is not necessary, simplifying accounting and ensuring safety for customers that want to make use of blockchain technology, without worrying about buying or holding cryptocurrency or tokens.

Identity Management

Baseledger's identity layer provides a compliance-centric balance between anonymity and accountability. A user's identity is anonymous on-chain, but this anonymity can be revoked and their real-world identity can be revealed in response to a valid request from an authority via established legal channels.

From the user's perspective, anonymity with respect to the general public is maintained and the identity layer can accommodate identity providers and

Archived copy · cryp2nova.com

anonymity revokers based in different jurisdictions around the world. As such, the Baseledger network offers a global, multi-jurisdictional solution to the adoption of blockchain technologies across regulatory regimes.

Baseledger includes a solution for providing transactional privacy for users, while maintaining accountability against local regulations. This means that transactions are processed without exposing the identity of the sender or receiver. In case of encrypted transfers, the sender and receiver are the only parties that can see the actual amount of a transaction. If a suspicious transaction or set of transactions is detected or in case of a legal conflict, the real-world identity of the users can be revealed to qualified authorities with the help of anonymity revokers and identity providers. Moreover, if a specific real-world identity is suspected of malicious behavior, anonymity revokers and identity providers can help trace the accounts of that user.

The elements of Baseledger's Identity architecture include *users*, *identity providers,* and *anonymity revokers*.

A **user** is an entity that holds an account on Baseledger. These can be individuals or legal entities, such as businesses, and they require a valid form of identification to facilitate the off-chain identification process.

An **identity provider** is a person or organization that performs off-chain identification of users. For each identity issued for a user the identity provider stores a record off-chain called an identity object. The primary functions of an identity provider are to:

- Verify the identity of users
- Issue user identity certificates to users
- Create and store identity objects and relevant attributes for record keeping purposes
- Participate in the anonymity revocation process

Information about the organizations that act as identity providers, such as their name, location or public key, is found in an on-chain registry. Initially, the registration of identity providers will be managed by the Baseledger Council. Users are required to

Archived copy · cryp2nova.com

obtain an identity object from an identity provider in order to open and operate an account on the network.

An **anonymity revoker** is a person or organization that is trusted by the council to help identify a user that owns an account should the need arise. All accounts on the are associated with a real-world identity, which is linked to an identity object stored by an identity provider. Identity objects are also linked to a set of anonymity revokers. Anonymity revokers play a critical role in revealing the real-world identity of a suspicious user by decrypting the unique user identifier that is stored on-chain for each account. When a unique user identifier has been decrypted in response to an official order, it can be combined with information stored by the relevant identity provider to allow the qualified authorities to reveal the real-world identity of the user.

From a big picture perspective, this approach allows Baseledger to offer a well-balanced compromise between (pseudo-)anonymity and a compliant way to revoke anonymity if needed (e.g., in case of legal fillings). This is another vital building block in offering an enterprise-grade, compliant solution for companies to build on DLT promises.



Archived copy · cryp2nova.com

6 Summary

■ Baseledger is a public-permissioned, council-governed blockchain network that fulfills the major requirements of enterprise organizations for participating in Baseline-enabled processes: A unified architecture ensuring service quality, data privacy and integration.

■ Baseledger supports enterprise blockchain as a pillar in digital transformation. It supports evolutionary and incremental improvements in trust and transparency across business ecosystems.

■ Baseledger is designed to drive value for all types of organizations.

■ Baseledger is designed to support a variety of uses cases, without technical or architectural limitations to specific verticals.

■ Baseledger understands integration as a key issue to all use cases and includes this in the core of the Baseledger Architecture of Architectures.

■ Baseledger is designed to leverage the advantages of public permissioned blockchain networks to address the major needs of enterprises.

■ Baseledger is designed to support the Baseline approach, enabling a production ready mainnet architecture at enterprise scale as outlined in the Baseline Protocol.

■ Baseledger is built around the main enterprise requirements for service quality, data privacy and integration.

■ Baseledger equips enterprise ecosystems with best-of-breed infrastructure for adopting the Baseline protocol using pluggable Layer 1 and Layer 2 consensus mechanisms.

Archived copy · cryp2nova.com

Special Thanks

We want to thank Kartheek Solipuram, Lucas Rodriquez Benitez, Tomasz Stanczak, Andreas Freund, Anais Ofranc, Sam Stokes, John Wolpert, Jack Wiering, Myron Rotter, the teams from Unibright, Provide, Finspot and the entire Baseline Protocol Community.

Disclaimer

This document constitutes general information only and may be updated. It also contains forward looking statements that are based on the beliefs and intentions of the authors, as well as certain assumptions made by and information available to them. Such statements, assumptions, and information are based on analysis and sources considered appropriate and reliable, but there is no assurance as to their accuracy or completeness.

This whitepaper is a technical and functional description of the presented concepts related to a ledger for *baselining* and on blockchain solutions in general. This document does not represent a prospectus of any sort. Nothing contained in this document constitutes investment, legal, or tax advice. The information or any opinion contained herein does not constitute a solicitation or an offer to buy or sell any securities, futures, options, or other financial instruments. Decisions based on information contained in this document are the sole responsibility of the reader. The content is provided "AS IS" and without warranties of any kind (either expressed or implied). To the fullest extent permissible pursuant to applicable law, any and all warranties, expressed, or implied, including, but not limited to, implied warranties of merchantability and fitness for a particular purpose, are disclaimed.

This document is Copyright © 2021 by Unibright IT GmbH, 55411 Bingen am Rhein, Germany and Provide Technologies Inc., a Georgia corporation. All rights reserved.

Unibright IT GmbH is the legal owner and operator of UBT and the UBT token model.

Providibright S.à R.L (Luxembourg) is the legal operator of the Provide Payments service when mentioned throughout this document.

Images from unsplash

dan-stark-DLwUVlzrP0Q

hugo-jehanne-LOHVrTsdvzY

jeremy-perkins-7S1yZoFcVV0

xan-griffin-eA2t5EvcxU4

xandtor-h1dmlM66Ta0

Archived copy · cryp2nova.com