Master Project Proposal Template

Adam Babs
adam.babs@uva.nl

January 2022

Legend:

1 Project details

Project title: Coordinating Multi-Domain Distributed Applications Using Hyperledger Blockchain and Petrinets Encoded Smart Contracts

Student Name: Adam Babs

Host organization or research group: Internal Project at the University of Amsterdam

Contact person: Dr. Reginald Cushing R.S.Cushing@uva.nl

Contents

2 Project summary

Global Context

The growth of programmable infrastructures combined with the the increasing value of data facilitates developing a new type of applications, namely, multi-domain applications. As Yuosre F. Badir et al. discuss, with globalization and the networked world of today, there is a dire need for a reliable and efficient model to manage, monitor, and control global large-scale projects, which contain thousands of workflows and hundreds of organizations located at different sites [1]. One of many examples of such multi-domain infrastructure is collaborative cyberattack defense in software-defined networking, where multiple parties share cyber threat intelligence to improve their security defense mechanisms against for instance DDOS attacks [2]. In this particular example, autonomous systems share blacklists containing for example malicious IP addresses. This process requires trust and mutual cooperation since the adversaries may gain awareness on the detection of their attack if the exchanged information is disclosed outside the trusted zone. Other use cases requiring multi-domain applications cooperation can be found here: `https://amdex.eu/usecases/` [3]. AMdEX is a field lab working on neutral exchange infrastructure that provides and executes reliable data sharing archetypes.

Distributed multi-domain applications give rise to multiple challenges such as lack of trust and single point of failure of the 3rd party coordinator, centralization of authority, and scalability limitations. On the contrary, the decentralization of cooperation between parties is associated with many challenges. How multi-lateral contracts can be encoded into enforceable/monitorable rules? How will multi-lateral contracts be enforced without a 3rd party? How will the coordination of multi-domain applications operate?

The main objective of this work is to model multi-domain coordination with an underlying infrastructure modeled as a set of Petrinets that will be deployed as smart contracts hence minimizing the role of an outside coordinator. Decentralization of the workflow and the whole process will be based on rules and policies mutually agreed by the participating organizations.

Research Questions

RQ1. *How can we use blockchain technology as a workflow coordination layer, modeled as a set of Petrinets, between multiple distributed applications, for the purpose of increasing scalability, improving safety, and eliminating the single point of failure problem?*

> **Sub-RQ.** *How can we generalize this approach of coupling blockchain with Petrinets to obtain a general architecture that will work on various applications that run on network containers?*

RQ2. *What are the benefits and drawbacks that accrue from combining blockchain and Petrinets to model the workflow between multiple distributed applications, instead of using centralized solutions?*

> **Sub-RQ.** *Juxtaposition of blockchain approach and a centralized approach and comparison of several metrics to illustrate the tradeoff between efficiency and fairness/trustworthiness. This will be evaluated against metrics presented in section 5.1*

3 Problem analysis

3.1 Why workflow decentralization?

Workflows are typically managed by Workflow Management Systems (WfMS), which consist of software components to create, direct, and monitor the execution of workflows. A WfMS provides support in two key areas: build-time and run-time functions. These functions always involve a large number of physically dispersed participants. In a conventional client–server-based workflow system, these dispersed participants interact with a centralized data repository (DR) and a centralized workflow engine with the assistance of client applications, requesting data and commands, respectively. Almost all the workflow functions are, thus, carried out on the server-side in a centralized manner. Unfortunately, such an approach has encountered many problems as follows described in [4, 5, 6].

From the point of view of this work the two most important drawbacks are the following:

1. Systems built on top of the client-server architecture are normally vulnerable to server failures. The centralized server is normally viewed as a single point of failure in the system. The malfunction of the server may bring the whole system down. Again, this deficiency is more evident in application domains where the workflow server is required to manage many workflow instances [7].

2. Limited scalability of the client-server architecture prevents WfMSs based on it from coping with the everchanging workflow environment. It also raises difficulties in system configuration, as any change to the system, e.g., joining of new participants, requires modifying and updating the centralized workflow server, which is very inconvenient and inefficient [7].

Moreover, as Yun Yan et al. the traditional client/server architecture for workflow has exhibited many weaknesses, as such an architecture seriously degrades system performance, greatly lacks scalability in a dynamic environment and rigidly restricts human beings [4].

3.2 Innovation

The main innovation of this project emerges from the combination of widely used tools from different fields for diverse purposes. One is a blockchain-based collaboration of parties to achieve a common goal while maintaining safe data exchange, decentralization, privacy, and scalability. The second one is modeling the workflow between multiple parties using Petrinets. The coupling of these two, might result in coordination of distributed multi-domain workflows without a 3rd party central control and strongly diminish the role of trusted 3rd parties that are needed to manage workflows such as for instance Apache Taverna [8].

3.3 Petrinets

To the best of our knowledge, there are no papers about combining the Petrinet models with blockchain to coordinate distributed multi-domain applications, however, these two tools have been often used together before for blockchain analysis [9], verification of smart contracts on blockchain [10] or generation of safe smart contracts based on petrinets models [11].

As Wil van der Aalst describes [12], Petrinets have a wide spectrum of possible applications in managing workflow systems and there are at least three good reasons for developing Petri-net-based workflow management systems. These are:

- Formal semantics, regardless of their graphical nature.
- State-based instead of event-based flow.
- Wide range of available analysis techniques and tools.

In later stages, the author proves that Petrinets can cover all requirements stated by the Workflow Management Coalition [13] that established standards to be used in workflow management. Furthermore, Petrinets facilitate state-based descriptions of WFMS which allows for a clear distinction between enabling of a task and the execution of a task, this has proven to be valuable in numerous projects. Lastly, there is an abundance of analysis techniques developed for Petrinets, enabling the user of a Petri-net-based WFMS to analyze a workflow process in various ways. There are many tools to simulate the workflow and analyze its, performance and structure at different angles.

Recently, Petrinets have been mainly considered as a modeling tool for workflow and work-flow systems [14, 15, 16]. There are a number of reasons [12, 17] for using a Petrinet-based approach in modeling and analyzing workflow systems. Petrinets allow a graphical representation to ease the understanding of the modeled system and at the same time, they can be used in formal analysis, verification, and validation of the model [18, 19, 20]. In a brief summary, different modeling techniques can be applied to workflow modeling, but Petrinets are the only formal techniques able to be used for both structural modeling and a wide range of qualitative and quantitative analysis [21].

3.4 Blockchain

Apart from all the hype that surrounds blockchain, it is a distributed-decentralized digital ledger offering a number of valuable and salient features. In the context of this project, the most important ones are scalability, privacy, and security of data.

The foundations of this technology are based on 4 pillars; ledger, smart contracts, consensus, and wallets. A ledger is a distributed immutable key-value store. Peer nodes involved in a blockchain, host a replica of the database which itself holds the ground truth. Being immutable, old values are not overwritten but updates are written as a new block which itself is hashed and linked to the next block of updates, hence creating the chain of blocks. Wallets are a PKI (Public Key Infrastructure) system whereby a user can only access the ledger using his keys and any writes to the ledger are recorded by the public key of the user. This in turn gives "ownership" of the record on the ledger using key signatures. Smart contracts are akin to web services but are hosted on the blockchain "overlay" network. The hosting of these services is replicated across the network and calls to a service function is called on all nodes in the network. If the output of the call is consistent amongst all peers then the call is deemed successful. This allows for deterministic temper proof code to execute by everyone instead of a central authority. Consensus is crucial since all peers are writing to the same ledger with the potential of breaking consistency and is needed to order the writes to the ledger [22].

As mentioned in sections before, one of the main concerns in relying on a 3rd party coordinator of the workflow is a single point of failure [23], if the coordinator fails, the whole workflow and cooperation between applications might be jeopardized. Due to the lack of central control and the decentralized nature of blockchain, the single point of failure problem is overcome [23], this is majorly important in systems like for instance: aircraft maintenance data market [3] or in situations where the failure of a centralized coordinator might put the cooperation of thousands of parties in danger like in the previously mentioned cyber attack defense [2].

3.5 Modelling Blockchain with Petrinets

For this project blockchain technology will provide handling and computation of data and authentication, whereas Petrinets will provide mechanisms to model and coordinate concurrent processes. The combination of these 2 concepts facilitates coordinating concurrent processes in a decentralized manner. Mapping a basic Petrinet to the blockchain is done by first creating a Petrinet definition on the ledger and then implementing functionality to move tokens and fire transitions. A Petrinet definition is created by first creating assets for the 3 basic elements (places, transition, tokens) and then creating an asset with the arcs connecting the places and transitions. Using the underlying public key infrastructure (PKI), the created assets are owned by the creator and can not be modified by other users until the creator transfers ownership. A multidomain Petrinet would include a net created by assets owned by different domains. Upon creating a net that includes multiple domains, each domain needs to accept the net by signing it. At this point the net becomes active. At any point, domains can revoke any net and hence making the net inactive.

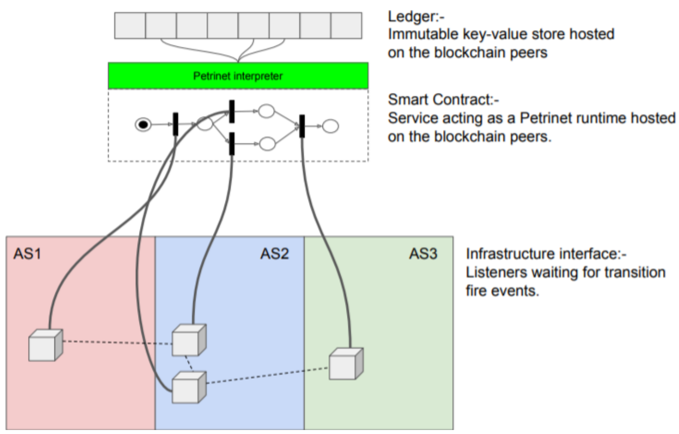

Figure 1: Interaction between the Petrinet layer and infrastructure layer. As the contract executes a Petrinet by moving tokens in places, transitions fire which generate events. These events are trapped by the infrastructure interface [22].

As shown in figure 1, interaction with the outside world occurs through blockchain events. A kind of publish-subscribe system on the blockchain. Firing events instruct the infrastructure to do a task and report back to the blockchain. At this point, the Petrinet executor decides to move the tokens to the output places [22].

4 Research method

The main hypothesis of this project is that through the use of chaincode and smart contracts, which execution would be linked and modeled as a set of Petrinets we can create a multi-domain workflow coordinator, ultimately decentralizing the whole process of cooperation between parties, based on mutually agreed cooperation policies and laws.

To prove this hypothesis, the main research method that is going to be employed during this project is Technical Action Research (TAR) [24]. In this research method, the goal of the researcher is to develop this artifact for use in a class of situations imagined by the researcher. Typically, then, the artifact is first tested, not on a real-world problem, but on toy problems under idealized circumstances in a laboratory. Next, it is scaled up to conditions of practice by solving more realistic problems with it, until it can be tested by using it in one or more concrete client organizations to solve concrete problems [24].

The exact same approach will be taken in this work. The first step is to implement the most simple architecture consisting of 2 peers that will exchange data with no policies and rules. Then, more components such as smart contracts, peer nodes, channels, organizations, places, transitions, edges, and tokens will be gradually added to achieve conditions that could potentially solve real-world problems.

Research for this project will begin with a precise analysis of the existing literature that overlaps the researched topic. A further profound investigation of what has already been done to get a broader view on what has been researched so in these areas so far. As indicated in previous sections, is some overlapping content that will be useful for the purpose of this project.

The main objective of further investigations will be gathering the input of the current knowledge in the fields of blockchain, Petrinets and workflow management systems and further, combining them in various configurations, see for instance [25], [26].

Ideally, the conducted research should be validated with a simulation of potential real-world use, similar to for instance adverting a DDoS attack [2] or enabling source routing. Furthermore, the worth of the proposed architecture should be proven in comparison to similar solutions that facilitate multi-domain distributed collaboration such as for instance Apache Taverna [8]. This will be done using metrics presented in section 5.1.

5 Expected results of the project

The following results are expected from this project:

1. A proof-of-concept architecture that can be applied to solve a potential real-world use-case.
2. A theoretical description of the applied methodology, together with a thorough analysis and illustration of each component, to illustrate its associated benefits and hindrances.
3. Juxtaposition of the proposed solution with a centralized approach, together with a comparison of advantages and disadvantages between the two, to illustrate the trade-off between efficiency, fairness/trustworthiness, and scalability.

5.1 Evaluation

The main cost of removing the authority is the complexity of a decentralized approach. Inevitably, the number of instructions and operations needed to execute a task on the blockchain instead of using a centralized approach will increase. It is a result of several limitations of smart contracts such as the need for data serialization and ordering, deterministic nature, and possible rights conflicts on the blockchain. There obviously is a number of variables to measure such as code complexity and volume to execute a single task, the number of transitions needed to execute the goal or time spent on execution, that will have an immense impact on the efficiency. In order to evaluate if the trade-off between decentralized and centralized approaches is beneficial, these metrics need to be compared. We suspect that more variables worth measuring will emerge along with the development of the project.

5.2 Metrics for Evaluation

There exists a number of general metrics to validate and evaluate the quality, performance, and scalability of blockchain application solutions such as [27]:

- Active Nodes
- Blocks Per Hour, Blocks Per Day

- Transactions Per Second
- Transaction Latency
- Transaction Throughput
- Full Node/Partial Node Ratio

Nonetheless, due to the nature of the described solution and coupling of blockchain with Petrinets, the expected evaluation will have to be more complex and take into consideration more aspects than just a single number indicating for instance the transaction throughput, as it will not provide valuable insight. As indicated before, along with the development of the project, important variables, or a combination of variables, to measure will emerge, and will be adjusted accordingly.

6 Required expertise for this project

Skills are measured on the following scale:

- Expert
- Advanced
- Intermediate
- Beginner

Skill	**Required Expertise**	**Current Expertise**
Hyperledger Fabric Technology	Advanced	Beginner
Petrinets Modelling	Intermediate	Intermediate
JavaScript Programming	Advanced	Advanced
Docker Container Orchestration & Management	Intermediate	Beginner

Table 1: Table of required expertise for the project

7 Timeline

The timeline can be found as a Gantt diagram as figure 2.

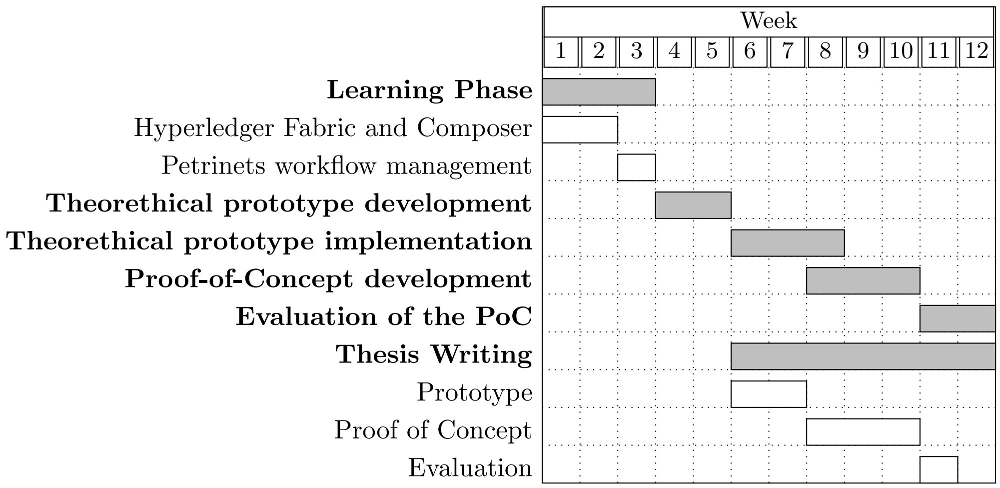

Figure 2: Gantt Chart Timeline

8 Risks

The gap between possessed expertise and the required expertise is too large.

To mitigate the possibility that this risk becomes reality and results in a fatal problem for the completion of the project, during the first phase of the project, the time has been allocated for knowledge gathering and learning key concepts and technologies. This is meant to reduce the gap between the required and current knowledge.

Proof-of-Concept will not yield the expected result.

The second biggest risk is that the project will not yield a proof-of-concept implementation or an insufficient one due to implementation difficulties or time constraints. This risk can be mitigated by extending the duration of the whole project.

Validation of the metrics

There exists a number of metrics to validate and evaluate the quality, performance, and scalability of blockchain application solutions as indicated before: [5.2]. However, due to the nature of the solution, based on coupling a number of solutions, a more sophisticated evaluation will have to be conducted as these metrics will not provide a valuable evaluation when presented singly, in isolation. A more refined evaluation will be conducted, taking into consideration a wider range of metrics, such as complexity, the number of transitions fired, code volume, and a number of instructions needed to execute a single task. Ideally, the solution will be benchmarked against a similar solution such as the Collaborative cyber attack defense in SDN networks using blockchain technology [2].

9 Literature survey

For the literature survey section, we have conducted research on various topics, listed below. For each of these research activities, the tool that has been mainly used is Google Scholar.
The majority of papers included in the literature survey are from 3 fields and particular sub-topics:

- Workflow management systems (WfMs)

  - Petrinets-based workflow management systems

- Petrinets modeling

  - Petrinets-based blockchain management

  - Modelling workflow management systems with Petrinets

- Blockchain-based solutions for decentralization, scalability or distributed collaboration

  - Decentralization of distributed multidomain application

  using blockchain-based solutions

- Mix of all the above in different combinations

- Research methods

Conducting the literature survey yielded a lot of valuable insight on matters related to the project. As it turns out, there are already, to some degree, similar solutions that combine blockchain and Petrinets modeling to perform various processes.

Undoubtedly, there is a lot of valuable knowledge and resources on the topic that can be utilized for the purpose of this project. The majority of papers are frequently cited conference and journal papers, which makes a solid foundation for the execution of the project.

Table below depicts a number of useful concepts and topics, correlated with the topic and goal of this project.

Concept	**Description**	**Papers**
Concept A	Blockchain-based collaboration for safe data exchange	[2]
Concept B	Petrinet-based workflow management framework for safe data exchange	[25]
Concept C	The Application of Petrinets to Workflow Management	[28], [12]
Concept D	Workflow Management Systems Evaluation	[29]
Concept E	Challenges and Limitations of Blockchain solutions in the Internet of Things	[30]
Concept F	Areas of possible applications accruing from combining blockchain solutions with Petrinets modeling	[9], [10], [11], [26]

Table 2: Table of concepts

References

[1] Yuosre F Badir, Remi Founou, Claude Stricker, and Vincent Bourquin. Management of global large-scale projects through a federation of multiple web-based workflow management systems. *Project Management Journal*, 34(3):40–47, 2003.

[2] Mehrdad Hajizadeh, Nima Afraz, Marco Ruffini, and Thomas Bauschert. Collaborative cyber attack defense in sdn networks using blockchain technology. In *2020 6th IEEE Conference on Network Softwarization (NetSoft)*, pages 487–492. IEEE, 2020.

[3] Usecases — amdex. `https://amdex.eu/usecases/`. (Accessed on 01/15/2022).

[4] Jun Yan, Yun Yang, and Gitesh K Raikundalia. A decentralised architecture for workflow support. In *Proc. 7th Int. Symposium on Future Soft. Technology (ISFST02), CD ISBN*, pages 4–916227, 2002.

[5] Giacomo Piccinelli, Anthony Finkelstein, and Scott Lane Williams. Service-oriented workflow: The dysco framework. In *Euromicro Conference*, pages 291–291. IEEE Computer Society, 2003.

[6] Gustavo Alonso, Divyakant Agrawal, Amr El Abbadi, and Carl Mohan. Functionality and limitations of current workflow management systems. *IEEE expert*, 12(5):105–111, 1997.

[7] Jun Yan, Yun Yang, and Gitesh K Raikundalia. Swindew-a p2p-based decentralized workflow management system. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, 36(5):922–935, 2006.

[8] Taverna - apache incubator. `https://incubator.apache.org/projects/taverna.html`. (Accessed on 02/06/2022).

[9] Andrea Pinna, Roberto Tonelli, Matteo Orrú, and Michele Marchesi. A petri nets model for blockchain analysis. *The Computer Journal*, 61(9):1374–1388, 2018.

[10] Zhentian Liu and Jing Liu. Formal verification of blockchain smart contract based on colored petri net models. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, volume 2, pages 555–560. IEEE, 2019.

[11] Nejc Zupan, Prabhakaran Kasinathan, Jorge Cuellar, and Markus Sauer. Secure smart contract generation based on petri nets. In *Blockchain Technology for Industry 4.0*, pages 73–98. Springer, 2020.

[12] Wil MP Van Der Aalst. Three good reasons for using a petri-net-based workflow management system. In *Information and Process Integration in Enterprises*, pages 161–182. Springer, 1998.

[13] David Hollingsworth and UK Hampshire. Workflow management coalition: The workflow reference model. *Document Number TC00-1003*, 19(16):224, 1995.

[14] van der Aalst Wil, Jörg Desel, and Andreas Oberweis. *Business process management: Models, techniques, and empirical studies*. Springer, 2003.

[15] WMP van der Aalst. Workflow management: net-based concepts, models, techniques, and tools (wfm'98): proceedings of the workshop, june 22, 1998, lisbon, portugal. 1998.

[16] Amit Sheth. Nsf workshop on workflow and process automation in information systems: state-of-the-art and future directions. *ACM SIGGROUP Bulletin*, 18(1):23–24, 1997.

[17] Clarence A Ellis and Gary J Nutt. Modeling and enactment of workflow systems. In *International Conference on Application and Theory of Petri Nets*, pages 1–16. Springer, 1993.

[18] Wil MP Van der Aalst. Verification of workflow nets. In *International Conference on Application and Theory of Petri Nets*, pages 407–426. Springer, 1997.

[19] Wil MP Van Der Aalst. Workflow verification: Finding control-flow errors using petri-net-based techniques. In *Business Process Management*, pages 161–183. Springer, 2000.

[20] Jörg Desel. Validation of process models by construction of process nets. In *Business Process Management*, pages 110–128. Springer, 2000.

[21] Khodakaram Salimifard and Mike Wright. Petri net-based modelling of workflow systems: An overview. *European journal of operational research*, 134(3):664–676, 2001.

[22] Cees de Laat Reginald Cushing. Paola Grosso. Petrinet smart contracts for multi-domain network collaboration, 2022.

[23] Ali Dorri, Salil S Kanhere, and Raja Jurdak. Blockchain in internet of things: challenges and solutions. *arXiv preprint arXiv:1608.05187*, 2016.

[24] Roel Wieringa and Ayşe Moralı. Technical action research as a validation method in information systems design science. In *International Conference on Design Science Research in Information Systems*, pages 220–238. Springer, 2012.

[25] Soraia Oueida and Yehia Kotb. A petrinet-based framework for healthcare blockchain systems. In *Proceedings of the Future Technologies Conference*, pages 573–587. Springer, 2021.

[26] Md Atik Shahriar, Faisal Haque Bappy, AKM Fakhrul Hossain, Dayamoy Datta Saikat, Md Sadek Ferdous, Mohammad Jabed M Chowdhury, and Md Zakirul Alam Bhuiyan. Modelling attacks in blockchain systems using petri nets. In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 1069–1078. IEEE, 2020.

[27] Blockchain metrics — arcitura patterns. `https://patterns.arcitura.com/blockchain-patterns/blockchain-metrics`.

[28] Wil MP Van der Aalst. The application of petri nets to workflow management. *Journal of circuits, systems, and computers*, 8(01):21–66, 1998.

[29] Jörg Lenhard, Vincenzo Ferme, Simon Harrer, Matthias Geiger, and Cesare Pautasso. Lessons learned from evaluating workflow management systems. In *International Conference on Service-Oriented Computing*, pages 215–227. Springer, 2017.

[30] Ali Dorri, Salil S Kanhere, and Raja Jurdak. Blockchain in internet of things: challenges and solutions. *arXiv preprint arXiv:1608.05187*, 2016.