1810 - Software example - consensus mechanism CRA 2018	
BENCHMARKS	**ACTIVITIES BY YEAR**
Internet searches: 17 Articles	FY2018
Competitive products or processes: 6 products	'1-1
	Activity 1
OBJECTIVES	**RESULTS**
Energy efficiency: 15 kw/h	25
Scalabilty: 100000000 # total nodes	110000000
Reduce redundant operations: 5 %	11
Achieve FAIR distribution among nodes: 95 % accuracy	97
Reduce message overhead: 40 %	23
UNCERTAINTIES & KEY VARIABLES	**CONCLUSIONS**
1 - Adapt backoff mechanism	
dynamicity (# of joins & leaves)	Y
neighbourhood size & definition	Y
number of nodes	Y
propogation radius	Y
single POW vs multiple blockchain channels	Y
	METHODS
Analysis	17
Trials	438
Prototypes	3
Lines of code	7300
	COSTS
Hours	1940
Materials $	
Subcontractor $	

Project Details:

Scientific or Technological Objectives:

Measurement	Current Performance	Objective	Has results?
Energy efficiency (kw/h)	50	15	Yes
Scalabilty (# total nodes)	1000000	100000000	Yes
Reduce redundant operations (%)	50	5	Yes
Achieve FAIR distribution among nodes (% accuracy)	80	95	Yes
Reduce message overhead (%)	100	40	Yes

NOTE: THIS PROJECT DESCRIPTION IS BASED ON THE CANADA REVENUE AGENCY EXAMPLE RELEASED OCTOBER 2018.

We are specialized in social media field. Our existing Social Media Platform was developed to allow users to gain cash rewards based on their contributions. We seek to reward them using cryptocurrency. For better market share, our objective was to develop a new cryptocurrency which will be more energy efficient than the existing cryptocurrencies.

Cryptocurrencies rely on Blockchain networks and use consensus mechanisms to validate financial transactions. Existing Proof of Work (PoW) consensus mechanism guarantees a fair distribution of mining chances but it suffers from an overall energy consumption issue since the validation operations are duplicated.
Enhancements to this consensus mechanism (e.g. using mining pools) or alternative mechanisms, such as Proof of Stake (PoS), can reduce the number of redundant operations, but result in a monopoly in terms of validation chances among miners.

We seek to achieve at least 30% reduction in the overall energy consumption without degrading fairness among miners. To do so, we thought about augmenting PoW by adding probabilistic behaviour to limit the access to transactions validation.

Field of Science/Technology:

Software engineering and technology (2.02.09)

Project Details:

Intended Results:	Develop new processes
Work locations:	Lab
Key Employees:	Software Developer (Unknown / Unknown)
Evidence types:	Progress reports, minutes of project meetings; Test protocols, test data, analysis of test results, conclusions; Records of resources allocated to the project, time sheets; Design, system architecture and source code; Records of trial runs

Scientific or Technological Advancement:

Uncertainty #1: Adapt backoff mechanism

We found that the backoff mechanism, used in wireless networks (WLANs) for medium access control, may be a candidate for such objective. This mechanism uses random timers to grant access to the channel in a distributed fashion while reducing the collision rate. Overall, all the nodes have equal chance to access the channel. Also, this mechanism adapts very well to network congestion.

Our idea was to transpose such behavior into Blockchain. Collisions (concurrent transmissions) in WLANs will mean duplicate validations in Blockchain. But, the backoff mechanism cannot be directly applied to Blockchain because, in WLANs, this mechanism is designed to share access to one channel, whereas in Blockchain we can have multiple transaction validations occurring simultaneously. Also, once a transaction is validated, there is no need for the backoff mechanism to be associated to this specific transaction.

Therefore, there is uncertainty in whether the backoff mechanism principles can be adapted to the specific nature of Blockchain networks and achieve the objective of processing transactions with minimal duplicates while keeping fairness among the nodes.

The most significant underlying key variables are:

number of nodes, dynamicity (# of joins & leaves), neighbourhood size & definition, single POW vs multiple blockchain channels, propogation radius

Technology or Knowledge Base Level:

Benchmarking methods & sources for citings:

Benchmark Method/Source	Measurement	Explanatory notes
Internet searches	17 Articles	examined differing uses and methods to deploy backoff mechanism
Competitive products or processes	6 products	examined collision mechanisms of 6 existing blockchain products

Activity #1-1: Activity 1 (Fiscal Year FY2018)

Methods of experimentation:

Method	Experimentation Performed
Analysis / simulation:	17 alternatives
Trials:	438 runs / samples
Physical prototypes:	3 samples
Lines of code:	7300 Lines of prototype code

From September to January, we thought about ways to apply the backoff mechanism principles to the overall Blockchain network.
One candidate solution was to create a variant of the backoff mechanism in which, when a new transaction is ready for validation, each set of nodes willing to validate that specific transaction will be considered as a separate channel and have a specific backoff mechanism attached to them. Thus, at a given point in time, multiple dynamic instances of the backoff mechanism will be running in parallel.

Moreover, in WLANs, the backoff mechanism relies on the capability of carrier sensing (CS) to perform its elementary timer operations (start, pause, resume, cancel), meaning that wireless nodes are able to sense if there is nearby activity.
In Blockchain, which relies on P2P topology, there is no way for a node to get a sense about the activity of the other nodes.
We thought about how we can emulate the lacking CS capability in P2P to allow miners to be informed about other mining activities. This is key to applying the principles of backoff mechanism to achieve our objectives.
Our idea was to create “regions” of miners allowing them to detect the level of localized mining activities within their neighborhood (a specific number of hops) and correctly apply the backoff timers operations only if the activity is related to the same transaction they want to validate.
The optimal neighborhood size has to be determined since the propagation of such information within a small (resp. large) neighborhood will result in less accurate emulation of CS, thus more collisions (resp. larger network messages overhead and bigger delays due to routing).

We wanted to validate through simulation the effectiveness of the use of the backoff mechanism as an enhancement to PoW. We called our new consensus mechanism Fairness of Work (FoW). We designed minimalistic models of PoW and FoW and implemented them in an open-source discrete-event simulator.
We defined parameters that will be used for input such as the number of nodes, the degree of dynamicity (joins/leaves) of the P2P network, the number of operations to validate, the neighborhood size, etc.
We also defined the performance metrics for evaluation of FoW against PoW, such as the number of redundant mining operations, the distribution of mining among the nodes and message overhead.
We then conducted many simulations, each with the same set of random conditions for both PoW and FoW.

Simulation results showed that the overall number of redundant mining operations was reduced by 40% while keeping a fair distribution of mining chance between miners. The performance of FoW starts to degrade when the size of the Blockchain network exceeds 200K nodes.

From February to June, we modified an open source Blockchain software client to include our new FoW mechanism. Then, we tested this mechanism using a small network in a real-world setting. Results were similar to simulation results, which validated the models used in the simulation and allowed us to create a model for PoS and run simulations to compare FoW against PoS without real-world settings.

Earlier work related to the integration of SMP with ccCoin and benchmarking of hardware mining devices to select the best candidate in terms of energy consumption was not claimed.

Results:

- Energy efficiency: 25 kw/h (71% of goal)
- Scalabilty: 110000000 # total nodes (110% of goal)
- Reduce redundant operations: 11 % (86% of goal)
- Achieve FAIR distribution among nodes: 97 % accuracy (113% of goal)
- Reduce message overhead: 23 % (128% of goal)

NOTE: THE IDEAL DESCRIPTION WOULD COMPARE RESULTS TO INITIAL GOALS & EXPECTATIONS THEN TRY TO EXPLAIN ANY VARIANCES.

Conclusion:

We have shown that the principles of the backoff mechanism, used for medium access control in WLANs to reduce frame collisions, can be applied to reduce energy consumption in Blockchain without creating mining monopoly.

We have found that dynamic instances of this mechanism can run in parallel and achieve the desired results. Also, it is possible to rely on partial information about transaction validation within regions of miners to emulate the carrier sensing capability. By combining both ideas, it is possible to reduce the number of mining operations within the overall Blockchain network.

Analysis of our experimental results shows that we can successfully reduce the amount of redundant mining operations by 40% while having a fair distribution of mining chance among miners. Our new mechanism, FoW, outperforms both the legacy PoW and PoS.

However, the results show that our FoW mechanism does not scale well for large Blockchain networks (beyond 200K active miners) due to the non-convergence of the propagation mechanism introduced to emulate the lack of carrier sensing capability. Increasing the propagation radius can possibly solve this problem for networks with low degree of dynamicity (join/leave).

Significant variables addressed: dynamicity (# of joins & leaves), neighbourhood size & definition, number of nodes, propogation radius, single POW vs multiple blockchain channels

Documentation:

- Offline Documents: Docs

Part 2 – Project information (continued)

Project number **1**

CRA internal form identifier 060
Code 1501

Complete a separate Part 2 for each project claimed this year.

Section A – Project identification

200 Project title (and identification code if applicable)

1810 - Software example - consensus mechanism CRA 2018

202 Project start date: 2018-02 (Year Month)

204 Completion or expected completion date: 2018-11 (Year Month)

206 Field of science or technology code (See guide for list of codes): 2.02.09 Software engineering and technology

Project claim history

208 1 ☐ Continuation of a previously claimed project **210** 1 ☐ First claim for the project

218 Was any of the work done jointly or in collaboration with other businesses? . . . . 1 ☐ Yes 2 ☐ No

If you answered **yes** to line 218, complete lines 220 and 221.

220 Names of the businesses	221 BN
1	

Section B – Project descriptions

242 What scientific or technological uncertainties did you attempt to overcome?
(*Maximum 50 lines*)

1. Objectives: Energy efficiency: Current performance is 50 kw/h, goal is 15
2. kw/h
3. Scalabilty: Current performance is 1000000 # total nodes, goal is 100000000 #
4. total nodes
5. Reduce redundant operations: Current performance is 50 %, goal is 5 %
6. Achieve FAIR distribution among nodes: Current performance is 80 % accuracy,
7. goal is 95 % accuracy
8. Reduce message overhead: Current performance is 100 %, goal is 40 %.
9. NOTE: THIS PROJECT DESCRIPTION IS BASED ON THE CANADA REVENUE AGENCY EXAMPLE
10. RELEASED OCTOBER 2018.
11. We are specialized in social media field. Our existing Social Media Platform
12. was developed to allow users to gain cash rewards based on their
13. contributions. We seek to reward them using cryptocurrency. For better market
14. share, our objective was to develop a new cryptocurrency which will be more
15. energy efficient than the existing cryptocurrencies.
16. Cryptocurrencies rely on Blockchain networks and use consensus mechanisms to
17. validate financial transactions. Existing Proof of Work (PoW) consensus
18. mechanism guarantees a fair distribution of mining chances but it suffers
19. from an overall energy consumption issue since the validation operations are
20. duplicated.
21. Enhancements to this consensus mechanism (e.g. using mining pools) or
22. alternative mechanisms, such as Proof of Stake (PoS), can reduce the number
23. of redundant operations, but result in a monopoly in terms of validation
24. chances among miners.
25. We seek to achieve at least 30% reduction in the overall energy consumption
26. without degrading fairness among miners. To do so, we thought about
27. augmenting PoW by adding probabilistic behaviour to limit the access to
28. transactions validation.
29. Uncertainty #1: Adapt backoff mechanism
30. We found that the backoff mechanism, used in wireless networks (WLANs) for
31. medium access control, may be a candidate for such objective. This mechanism
32. uses random timers to grant access to the channel in a distributed fashion
33. while reducing the collision rate. Overall, all the nodes have equal chance
34. to access the channel. Also, this mechanism adapts very well to network
35. congestion.
36. Our idea was to transpose such behavior into Blockchain. Collisions
37. (concurrent transmissions) in WLANs will mean duplicate validations in

242 What scientific or technological uncertainties did you attempt to overcome?
(*Maximum 50 lines*)

Blockchain. But, the backoff mechanism cannot be directly applied to Blockchain because, in WLANs, this mechanism is designed to share access to one channel, whereas in Blockchain we can have multiple transaction validations occurring simultaneously. Also, once a transaction is validated, there is no need for the backoff mechanism to be associated to this specific transaction.

Therefore, there is uncertainty in whether the backoff mechanism principles can be adapted to the specific nature of Blockchain networks and achieve the objective of processing transactions with minimal duplicates while keeping fairness among the nodes.

Key variables: number of nodes, dynamicity (# of joins & leaves), neighbourhood size & definition, single POW vs multiple blockchain channels, propogation radius

244 What work did you perform **in the tax year** to overcome the scientific or technological uncertainties described in line 242?
(Summarize the systematic investigation or search) (*Maximum 100 lines*)

Activity: Activity 1

Methods of experimentation:Analysis / simulation:17 runs / samples, Trials:438 alternatives, Physical prototypes:3 samples, Lines of code:7300 Lines of prototype code

From September to January, we thought about ways to apply the backoff mechanism principles to the overall Blockchain network.

One candidate solution was to create a variant of the backoff mechanism in which, when a new transaction is ready for validation, each set of nodes willing to validate that specific transaction will be considered as a separate channel and have a specific backoff mechanism attached to them.

Thus, at a given point in time, multiple dynamic instances of the backoff mechanism will be running in parallel.

Moreover, in WLANs, the backoff mechanism relies on the capability of carrier sensing (CS) to perform its elementary timer operations (start, pause, resume, cancel), meaning that wireless nodes are able to sense if there is nearby activity.

In Blockchain, which relies on P2P topology, there is no way for a node to get a sense about the activity of the other nodes.

We thought about how we can emulate the lacking CS capability in P2P to allow miners to be informed about other mining activities. This is key to applying the principles of backoff mechanism to achieve our objectives.

Our idea was to create regions of miners allowing them to detect the level of localized mining activities within their neighborhood (a specific number of hops) and correctly apply the backoff timers operations only if the activity is related to the same transaction they want to validate.

The optimal neighborhood size has to be determined since the propagation of such information within a small (resp. large) neighborhood will result in less accurate emulation of CS, thus more collisions (resp. larger network messages overhead and bigger delays due to routing).

We wanted to validate through simulation the effectiveness of the use of the backoff mechanism as an enhancement to PoW. We called our new consensus mechanism Fairness of Work (FoW). We designed minimalistic models of PoW and FoW and implemented them in an open-source discrete-event simulator.

We defined parameters that will be used for input such as the number of nodes, the degree of dynamicity (joins/leaves) of the P2P network, the number of operations to validate, the neighborhood size, etc.

We also defined the performance metrics for evaluation of FoW against PoW, such as the number of redundant mining operations, the distribution of mining among the nodes and message overhead.

We then conducted many simulations, each with the same set of random conditions for both PoW and FoW.

Simulation results showed that the overall number of redundant mining

244 What work did you perform **in the tax year** to overcome the scientific or technological uncertainties described in line 242? (Summarize the systematic investigation or search) (*Maximum 100 lines*)

43. operations was reduced by 40% while keeping a fair distribution of mining
44. chance between miners. The performance of FoW starts to degrade when the size
45. of the Blockchain network exceeds 200K nodes.
46. From February to June, we modified an open source Blockchain software client
47. to include our new FoW mechanism. Then, we tested this mechanism using a
48. small network in a real-world setting. Results were similar to simulation
49. results, which validated the models used in the simulation and allowed us to
50. create a model for PoS and run simulations to compare FoW against PoS without
51. real-world settings.
52. Earlier work related to the integration of SMP with ccCoin and benchmarking
53. of hardware mining devices to select the best candidate in terms of energy
54. consumption was not claimed.

246 What scientific or technological advancements did you achieve or attempt to achieve as a result of the work described in line 244? (*Maximum 50 lines*)

1. Activity: Activity 1
2. Results: Result vs. Expectations
3. Energy efficiency (kw/h) 25 71%
4. Scalabilty (# total nodes) 110000000 110%
5. Reduce redundant operations (%) 11 86%
6. Achieve FAIR distribution among nodes (% accuracy) 97 113%
7. Reduce message overhead (%) 23 128%
8. NOTE: THE IDEAL DESCRIPTION WOULD COMPARE RESULTS TO INITIAL GOALS &
9. EXPECTATIONS THEN TRY TO EXPLAIN ANY VARIANCES.
10. Conclusion: We have shown that the principles of the backoff mechanism, used
11. for medium access control in WLANs to reduce frame collisions, can be applied
12. to reduce energy consumption in Blockchain without creating mining monopoly.
13. We have found that dynamic instances of this mechanism can run in parallel
14. and achieve the desired results. Also, it is possible to rely on partial
15. information about transaction validation within regions of miners to emulate
16. the carrier sensing capability. By combining both ideas, it is possible to
17. reduce the number of mining operations within the overall Blockchain network.
18. Analysis of our experimental results shows that we can successfully reduce
19. the amount of redundant mining operations by 40% while having a fair
20. distribution of mining chance among miners. Our new mechanism, FoW,
21. outperforms both the legacy PoW and PoS.
22. However, the results show that our FoW mechanism does not scale well for
23. large Blockchain networks (beyond 200K active miners) due to the non-
24. convergence of the propagation mechanism introduced to emulate the lack of
25. carrier sensing capability. Increasing the propagation radius can possibly
26. solve this problem for networks with low degree of dynamicity (join/leave).
27. Significant variables addressed: dynamicity (# of joins & leaves),
28. neighbourhood size & definition, number of nodes, propogation radius, single
29. POW vs multiple blockchain channels

Section C – Additional project information

Who prepared the responses for Section B?

253 1 [X] Employee directly involved in the project	254 Name: Developer, Software
255 1 [ ] Other employee of the company	256 Name
257 1 [ ] External consultant	258 Name / 259 Firm

List the key individuals directly involved in the project and indicate their qualifications/experience.

260 Names	261 Qualifications/experience and position title
1 Software Developer	BMath/ practicing since 2007
2	
3	

265 Are you claiming any salary or wages for SR&ED performed outside Canada? . . . . 1 [ ] Yes 2 [X] No

266 Are you claiming expenditures for SR&ED carried out on behalf of another party? . . . . 1 [ ] Yes 2 [X] No

267 Are you claiming expenditures for SR&ED performed by people other than your employees? . . . . 1 [ ] Yes 2 [X] No

If you answered **yes** to line 267, complete lines 268 and 269.

268 Names of individuals or companies	269 BN
1	

What evidence do you have to support your claim? (Check any that apply)
You do not need to submit these items with the claim. However, you are required to retain them in the event of a review.

- 270 1 [ ] Project planning documents
- 271 1 [X] Records of resources allocated to the project, time sheets
- 272 1 [ ] Design of experiments
- 273 1 [ ] Project records, laboratory notebooks
- 274 1 [X] Design, system architecture and source code
- 275 1 [X] Records of trial runs
- 276 1 [X] Progress reports, minutes of project meetings
- 277 1 [X] Test protocols, test data, analysis of test results, conclusions
- 278 1 [ ] Photographs and videos
- 279 1 [ ] Samples, prototypes, scrap or other artefacts
- 280 1 [ ] Contracts
- 281 1 [ ] Others, specify 282

RDBASE.NET T661 Tax Forms **RDBASE demo Canada**

Status | R&D form - Projects | Costs | Credits | Export to Tax Software

Enhancements to this consensus mechanism (e.g. using mining pools) or
alternative mechanisms, such as Proof of Stake (PoS), can reduce the number of redundant operations, but result in a monopoly in terms of validation chances among miners.

We seek to achieve at least 30% reduction in the overall energy consumption without degrading fairness among miners. To do so, we thought about augmenting PoW by adding probabilistic behaviour to limit the access to transactions validation.

Uncertainty #1: Adapt backoff mechanism

We found that the backoff mechanism, used in wireless networks (WLANs) for medium access control, may be a candidate for such objective. This mechanism uses random timers to grant access to the channel in a distributed fashion while reducing the collision rate. Overall, all the nodes have equal chance to access the channel. Also, this mechanism adapts very well to network congestion.

Our idea was to transpose such behavior into Blockchain. Collisions (concurrent transmissions) in WLANs will mean duplicate validations in Blockchain. But, the backoff mechanism cannot be directly applied to Blockchain because, in WLANs, this mechanism is designed to share access to one channel, whereas in Blockchain we can have multiple transaction validations occurring simultaneously. Also, once a transaction is validated, there is no need for the backoff mechanism to be associated to this specific transaction.

Therefore, there is uncertainty in whether the backoff mechanism principles can be adapted to the specific nature of Blockchain networks and achieve the objective of processing transactions with minimal duplicates while keeping fairness among the nodes.

Key variables: number of nodes, dynamicity (# of joins & leaves), neighbourhood size & definition, single POW vs multiple blockchain channels, propogation radius

Internet searches: 17 Articles -- examined differing uses and methods to deploy backoff mechanism

Competitive products or processes: 6 products -- examined collision mechanisms of 6 existing blockchain products

Note: based on word limits the following information did NOT get entered into the project description

244 What work did you perform **in the tax year** to overcome the scientific or technological uncertainties described in Line 242?(Summarize the systematic ir

Activity: Activity 1

Methods of experimentation:Analysis / simulation:17 runs / samples,