From Blockchain Research to Production Network

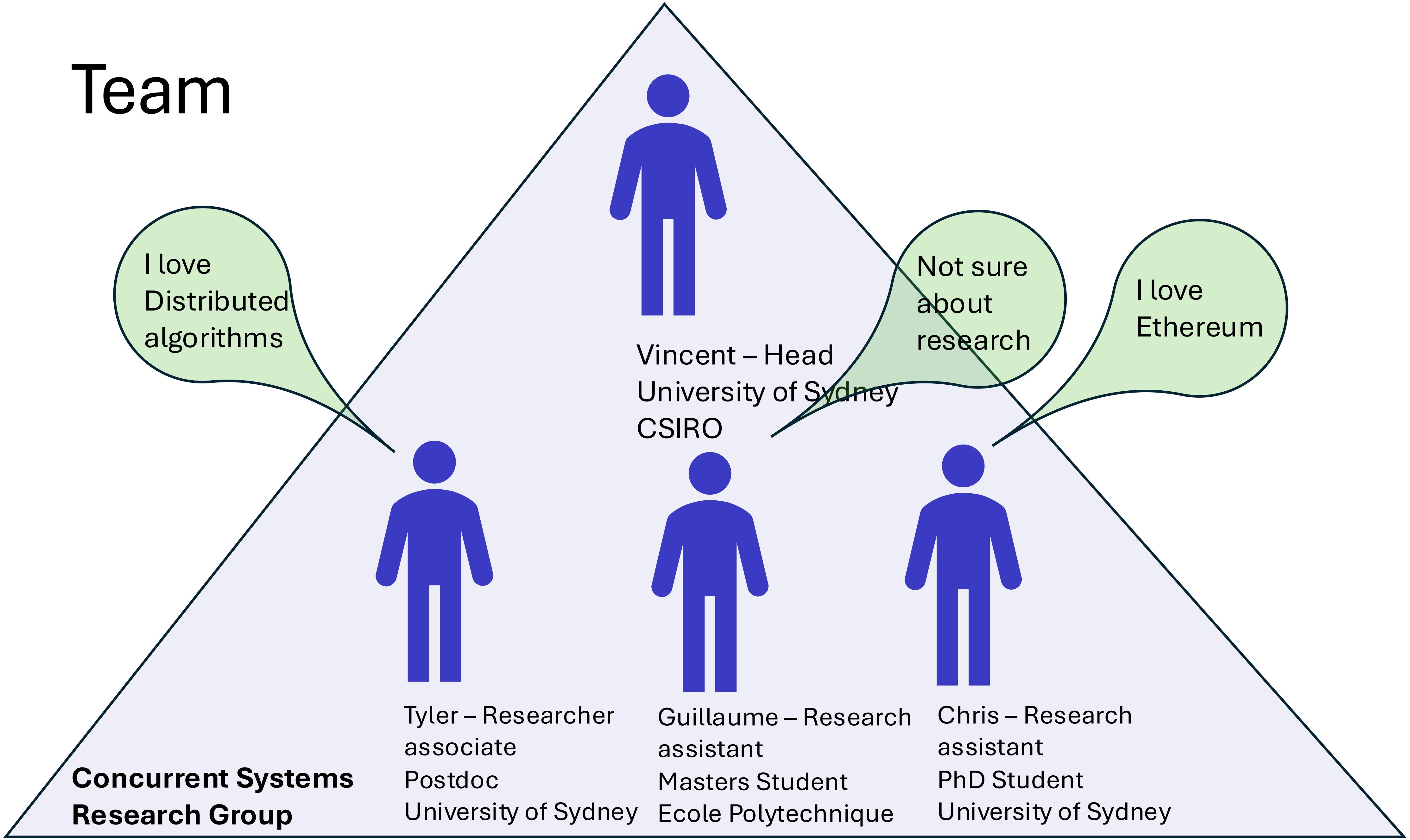
Vincent Gramoli

University of Sydney

Redbelly Network

Genesys

Team


I love Distributed algorithms
Vincent – Head
University of Sydney
CSIRO
Not sure about research
I love Ethereum
Tyler – Researcher associate
Postdoc
University of Sydney
Guillaume – Research assistant
Masters Student
Ecole Polytechnique
Chris – Research assistant
PhD Student
University of Sydney
Concurrent Systems Research Group

Intellectual Property

- CSIRO – Commercialisation Party
- University of Sydney – IP owner
- Inventors: Vincent, Tyler, Chris, Guillaume

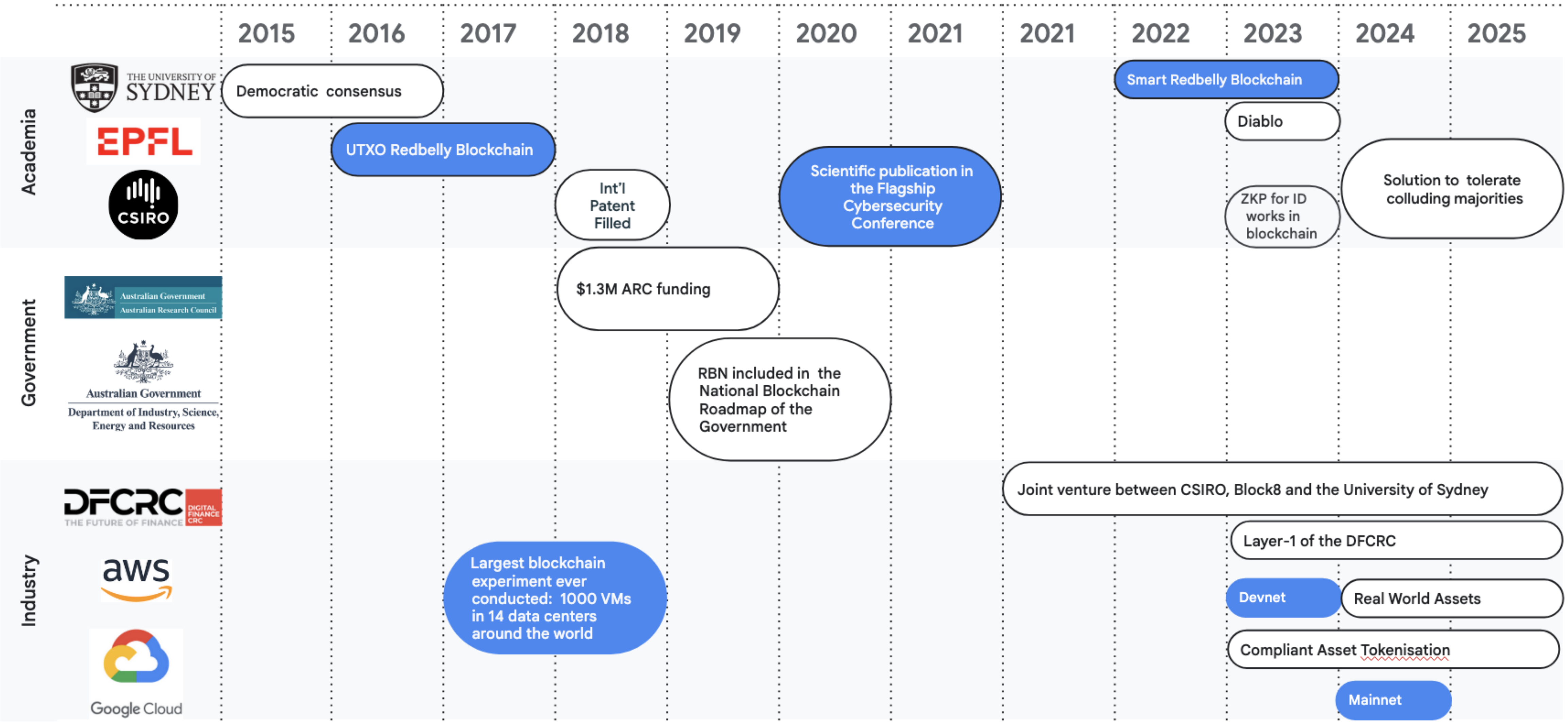
Commercialisation Strategies

1. Put it in the public domain
   - Not in the interest of the IP owner (University of Sydney)
   - May reduce value of the invention

2. Get a licence to find customers
   - Very easy in the US
   - Very hard in Australia

3. Sell the IP
   - **Cost a lot of money**
   - **Buyer is free to use as they wish**

Milestones



2015
2016
2017
2018
2019
2020
2021
2021
2022
2023
2024
2025
Academia
Government
Industry
Democratic consensus
UTXO Redbelly Blockchain
Int'l Patent Filled
Scientific publication in the Flagship Cybersecurity Conference
Smart Redbelly Blockchain
Diablo
ZKP for ID works in blockchain
Solution to tolerate colluding majorities
$1.3M ARC funding
RBN included in the National Blockchain Roadmap of the Government
Largest blockchain experiment ever conducted: 1000 VMs in 14 data centers around the world
Joint venture between CSIRO, Block8 and the University of Sydney
Layer-1 of the DFCRC
Devnet
Real World Assets
Compliant Asset Tokenisation
Mainnet

Accelerator

ON Program - CSIRO

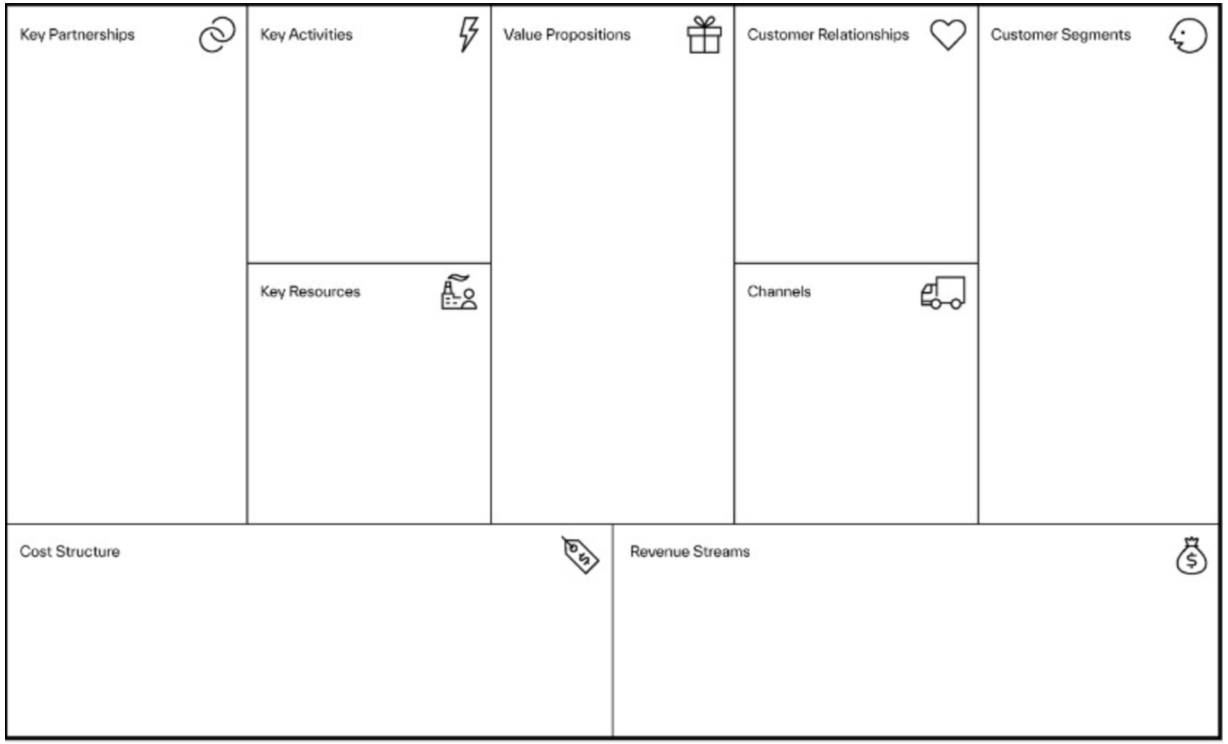
- The *ON Program* is centred on equipping researchers with the entrepreneurial and commercialisation skills they need to help them engage with business and drive greater uptake of their research and ideas.

- *ON Prime* - This nine-week program will help you develop the skills and confidence you need to undertake customer discovery and market validation activities. In ON Prime we work with researchers at any stage of their project who are exploring all pathways to impact.

ON Program - CSIRO

- How to communicate an elevator pitch
- How to write a pitch deck
- How to write a business model

=> I won a prize



Incubator

Incubate – The University of Sydney

- Teamed up with a mentor
- Learned how to harass prospects
- Did some homeworks (weekly meetings)

=> I learned my limits

Networking

Networking

- Go to meetups, events, conferences
- Meet the industry
- Understand the industry pain points
- Be patient with government

Redbelly Blockchain (2018)

- Creation of the company Redbelly Blockchain
- Vincent – CEO
- Partner – Kosmos Ventures
- CSIRO did not want to sell the IP to this partnership

Academic Journey

1. Finding Vulnerabilities (2015)

- We hacked Ethereum PoW
- We inform R3 consortium of financial institutions
- We hacked Ethereum PoA
- We informed CBA
- We are invited by Ethereum at the community conference

2. Finding a Fix (2016)

- We design the DBFT consensus algorithm
- We publish it at IEEE NCA 2018

operation bin_propose(v_i) **is**
$est_i \leftarrow v_i$; $r_i \leftarrow 0$;
while (true) **do**
  $r_i \leftarrow r_i + 1$;
  BV_broadcast $\text{EST}[r_i](est_i)$; // *add to $bin\_values[r_i]$ upon BV_delivery*
  wait_until $\big(bin\_values_i[r_i] \neq \emptyset\big)$;
  broadcast $\text{AUX}[r_i](bin\_values_i[r_i])$;
  wait_until $\big($messages $\text{AUX}[r_i](b\_val_{p(1)})$, ..., $\text{AUX}[r_i](b\_val_{p(n-t)})$ have been received
    from $(n-t)$ different processes $p(x)$, $1 \leq x \leq n-t$, and their contents are
    such that $\exists$ a non-empty set $values_i$ where (i) $values_i = \cup_{1 \leq x \leq n-t} b\_val_{p(x)}$
    and (ii) $values_i \subseteq bin\_values_i[r_i]\big)$;
  $b_i \leftarrow r_i$ mod 2;
  if $(values_i = \{v\})$ // *$values_i$ is a singleton whose element is v*
    then $est_i \leftarrow v$; **if** $(v = b_i)$ **then** decide(v) if not yet done **end if**;
    else $est_i \leftarrow b_i$
  end if;
end while.

when $\text{B-VAL}[r](v)$ is **BV-delivered** by BV_broadcast[r] **do**
  $bin\_values_i[r] \leftarrow bin\_values_i[r] \cup \{v\}$;

DBFT: Efficient Leaderless Byzantine Consensus and its Application to Blockchains

Tyler Crain and Vincent Gramoli
University of Sydney
Australia
{*tyler.crain,vincent.gramoli*}*@sydney.edu.au*

Mikel Larrea
Univ. of the Basque Country UPV/EHU
Spain
mikel.larrea@ehu.eus

Michel Raynal
Université de Rennes, France
Polytechnic University, Hong Kong
raynal@inria.fr

***Abstract*—This paper introduces a new leaderless Byzantine consensus called the *Democratic Byzantine Fault Tolerance (DBFT)* for blockchains. While most blockchain consensus protocols rely on a correct leader or coordinator to terminate, our algorithm can terminate even when its coordinator is faulty.**

The key idea is to allow processes to complete asynchronous rounds as soon as they receive a threshold of messages, instead of having to wait for a message from a coordinator that may be slow. The resulting decentralization is particularly appealing for blockchains for two reasons: *(i)* each node plays a similar role in the execution of the consensus, hence making the decision inherently "democratic"; *(ii)* decentralization avoids bottlenecks by balancing the load, making the solution scalable.

DBFT is deterministic, assumes partial synchrony, is resilience optimal, time optimal and does not need signatures. We first present a simple safe binary Byzantine consensus algorithm, modify it to ensure termination, and finally present an optimized reduction from multivalue consensus to binary consensus whose fast path terminates in 4 message delays.

***Index Terms*—Byzantine consensus, weak coordinator, geo-distribution**

I. Introduction and Related Work

To circumvent the impossibility of solving consensus in asynchronous message-passing systems [22] where processes can be faulty or *Byzantine* [30], researchers typically use randomization [3], [6], [14] or additional synchrony assumptions. Randomized algorithms can use per-process "local" coins or a shared "common" coin to solve consensus probabilistically among n processes despite $t < \frac{n}{3}$ Byzantine processes. When based on local coins, the existing algorithms converge in $O(n^{2.5})$ expected time [26]. A recent randomized algorithm without signature [34] solves consensus in $O(1)$ expected time under a fair scheduler. The fair scheduler assumption was later relaxed in an extended version [35] that we refer to as *Coin* in the remainder of the paper. Unfortunately, implementing a common coin increases the message complexity of the consensus algorithm.

To avoid the need of a common coin and solve the consensus problem *deterministically*, researchers have assumed partial or eventual synchrony [21]. Interestingly, these solutions typically require a unique *coordinator*, or leader, to be non-faulty [4], [8], [15], [20], [21], [27], [31], [32]. The advantage is that if the coordinator is non-faulty and if the messages are delivered in a timely manner in an asynchronous round, then the coordinator broadcasts its proposal to all processes and this value is decided after a constant number of message delays. The well-known drawback of this approach is that a faulty coordinator can dramatically impact the algorithm performance [1], [5], [17] by leveraging the power it has in a round and imposing its value to all.

In this paper, we present *Democratic Byzantine Fault Tolerance (DBFT)*, a Byzantine consensus algorithm that copes with this problem by not relying on a classic coordinator or leader. Instead, DBFT uses what we refer to as a *weak coordinator* that does not impose its value. On the one hand, this allows non-faulty processes to decide a value quickly without the help of the coordinator. On the other hand, the coordinator helps the algorithm terminating if non-faulty processes know that they proposed values that might all be decided. Furthermore, having a weak coordinator allows rounds to be executed optimistically without waiting for a specific message. Finally, DBFT is time optimal, resilience optimal and does not need signatures.

To mitigate the limitations of leader-based Byzantine consensus, other approaches were previously explored. Some protocols progressively reduce the time allocated to a coordinator to solve consecutive consensus instances in order to force the change of a slow coordinator [5], [17]. While this still requires a classic coordinator in each round, it favors the fastest coordinator in successive rounds. An exponential information gathering tree was used to terminate in $t + 3$ rounds without a coordinator [9]. Other solutions [21], [43] require at least $O(t)$ rounds. By contrast our weak coordinator only helps agreement by suggesting a value while still allowing a fast path termination in a constant number of message delays, hence differing from the classic coordinator [16], [21] or the eventual leader approaches that cannot be implemented in $\mathcal{BAMP}_{n,t}[t < n/3]$.

Application to blockchains. To motivate our algorithm, we study its applicability to the recent context of *blockchains* [37]. Blockchains originally aimed at tracking ownerships of digital assets where any Internet user could solve a cryptopuzzle before proposing, for consensus, a block of asset transactions. New blockchain models became promising at reducing the amount of resources consumed by avoiding to resolve the cryptopuzzle but restricting the set of proposers to a subset

2. Building a Blockchain PoC (2017)

- We extend DBFT
- Unspent Transaction Outputs (UTXO) model
- Signature verifications

3. Largest Blockchain Experiment

- 1000 machines
- 660,000 TPS
- 3s avg latency
- 11 countries

3. Largest Blockchain Experiment

- We used all the 14 availability zones of Amazon Web Services (AWS)
- AWS suspected a DoS attacks from us, they banned us
- I had to call my friends at AWS research to re-enable our account
- They decided to do a press release to talk about our results in the media

4. Idea Dissemination (2017)

Silvio Micali publishes Algorand few months later

- Presentation at MIT, Cambridge MA, USA

Facebook launches the Diem blockchain one year later

- Presentation at Facebook – Menlo Park, CA, USA

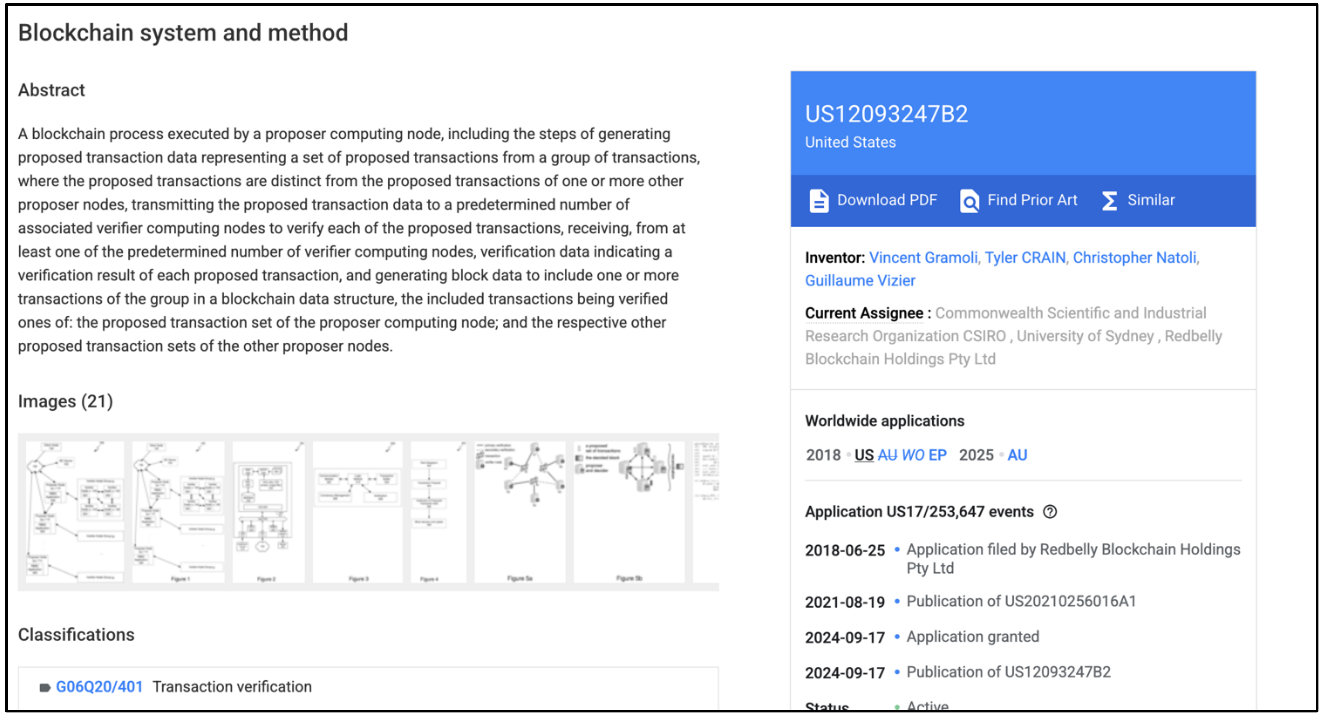
Visa publishes RapidChain one year later

- Presentation at Visa Research – Palo Alto, CA, USA

…

4. Patent (2018-2024)

- Submitted in 2018
- Described:
  - Superblock optimisations
  - Verification sharding
- Approved in 2024 in the US

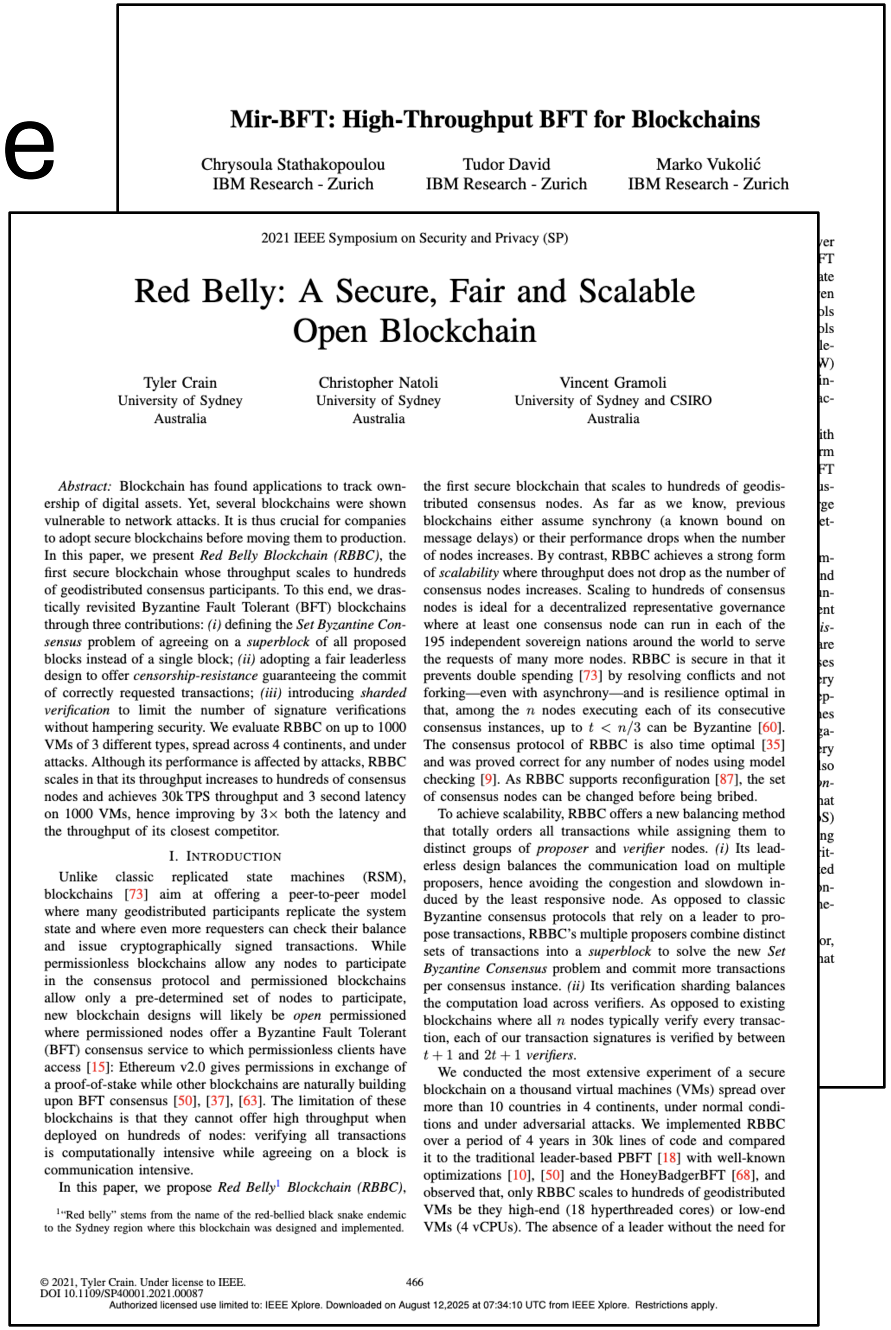


4. National Roadmap (2020)

- 1000 machines
- 660,000 TPS
- 3s avg latency

3. Flagship Security Conference

- The paper gets rejected many times
- We improved a lot and did not give up
- IBM releases a draft with similar ideas
- Redbelly gets published in IEEE S&P 2021



Mir-BFT: High-Throughput BFT for Blockchains

Chrysoula Stathakopoulou, IBM Research - Zurich
Tudor David, IBM Research - Zurich
Marko Vukolić, IBM Research - Zurich

2021 IEEE Symposium on Security and Privacy (SP)

Red Belly: A Secure, Fair and Scalable Open Blockchain

Tyler Crain, University of Sydney, Australia
Christopher Natoli, University of Sydney, Australia
Vincent Gramoli, University of Sydney and CSIRO, Australia

Abstract: Blockchain has found applications to track ownership of digital assets. Yet, several blockchains were shown vulnerable to network attacks. It is thus crucial for companies to adopt secure blockchains before moving them to production. In this paper, we present *Red Belly Blockchain (RBBC)*, the first secure blockchain whose throughput scales to hundreds of geodistributed consensus participants. To this end, we drastically revisited Byzantine Fault Tolerant (BFT) blockchains through three contributions: *(i)* defining the *Set Byzantine Consensus* problem of agreeing on a *superblock* of all proposed blocks instead of a single block; *(ii)* adopting a fair leaderless design to offer *censorship-resistance* guaranteeing the commit of correctly requested transactions; *(iii)* introducing *sharded verification* to limit the number of signature verifications without hampering security. We evaluate RBBC on up to 1000 VMs of 3 different types, spread across 4 continents, and under attacks. Although its performance is affected by attacks, RBBC scales in that its throughput increases to hundreds of consensus nodes and achieves 30k TPS throughput and 3 second latency on 1000 VMs, hence improving by 3× both the latency and the throughput of its closest competitor.

I. Introduction

Unlike classic replicated state machines (RSM), blockchains [73] aim at offering a peer-to-peer model where many geodistributed participants replicate the system state and where even more requesters can check their balance and issue cryptographically signed transactions. While permissionless blockchains allow any nodes to participate in the consensus protocol and permissioned blockchains allow only a pre-determined set of nodes to participate, new blockchain designs will likely be *open* permissioned where permissioned nodes offer a Byzantine Fault Tolerant (BFT) consensus service to which permissionless clients have access [15]: Ethereum v2.0 gives permissions in exchange of a proof-of-stake while other blockchains are naturally building upon BFT consensus [50], [37], [63]. The limitation of these blockchains is that they cannot offer high throughput when deployed on hundreds of nodes: verifying all transactions is computationally intensive while agreeing on a block is communication intensive.

In this paper, we propose *Red Belly*[1] *Blockchain (RBBC)*, the first secure blockchain that scales to hundreds of geodistributed consensus nodes. As far as we know, previous blockchains either assume synchrony (a known bound on message delays) or their performance drops when the number of nodes increases. By contrast, RBBC achieves a strong form of *scalability* where throughput does not drop as the number of consensus nodes increases. Scaling to hundreds of consensus nodes is ideal for a decentralized representative governance where at least one consensus node can run in each of the 195 independent sovereign nations around the world to serve the requests of many more nodes. RBBC is secure in that it prevents double spending [73] by resolving conflicts and not forking—even with asynchrony—and is resilience optimal in that, among the n nodes executing each of its consecutive consensus instances, up to $t < n/3$ can be Byzantine [60]. The consensus protocol of RBBC is also time optimal [35] and was proved correct for any number of nodes using model checking [9]. As RBBC supports reconfiguration [87], the set of consensus nodes can be changed before being bribed.

To achieve scalability, RBBC offers a new balancing method that totally orders all transactions while assigning them to distinct groups of *proposer* and *verifier* nodes. *(i)* Its leaderless design balances the communication load on multiple proposers, hence avoiding the congestion and slowdown induced by the least responsive node. As opposed to classic Byzantine consensus protocols that rely on a leader to propose transactions, RBBC's multiple proposers combine distinct sets of transactions into a *superblock* to solve the new *Set Byzantine Consensus* problem and commit more transactions per consensus instance. *(ii)* Its verification sharding balances the computation load across verifiers. As opposed to existing blockchains where all n nodes typically verify every transaction, each of our transaction signatures is verified by between $t+1$ and $2t+1$ *verifiers*.

We conducted the most extensive experiment of a secure blockchain on a thousand virtual machines (VMs) spread over more than 10 countries in 4 continents, under normal conditions and under adversarial attacks. We implemented RBBC over a period of 4 years in 30k lines of code and compared it to the traditional leader-based PBFT [18] with well-known optimizations [10], [50] and the HoneyBadgerBFT [68], and observed that, only RBBC scales to hundreds of geodistributed VMs be they high-end (18 hyperthreaded cores) or low-end VMs (4 vCPUs). The absence of a leader without the need for

[1] "Red belly" stems from the name of the red-bellied black snake endemic to the Sydney region where this blockchain was designed and implemented.

© 2021, Tyler Crain. Under license to IEEE.
DOI 10.1109/SP40001.2021.00087
466
Authorized licensed use limited to: IEEE Xplore. Downloaded on August 12,2025 at 07:34:10 UTC from IEEE Xplore. Restrictions apply.

MVP

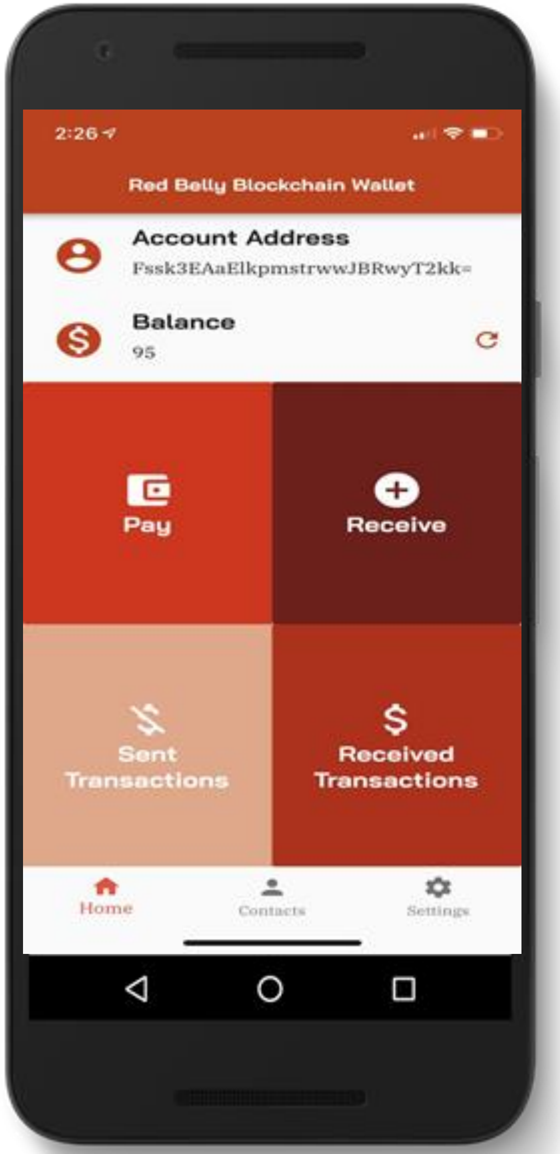
Minimum Viable Product

Development

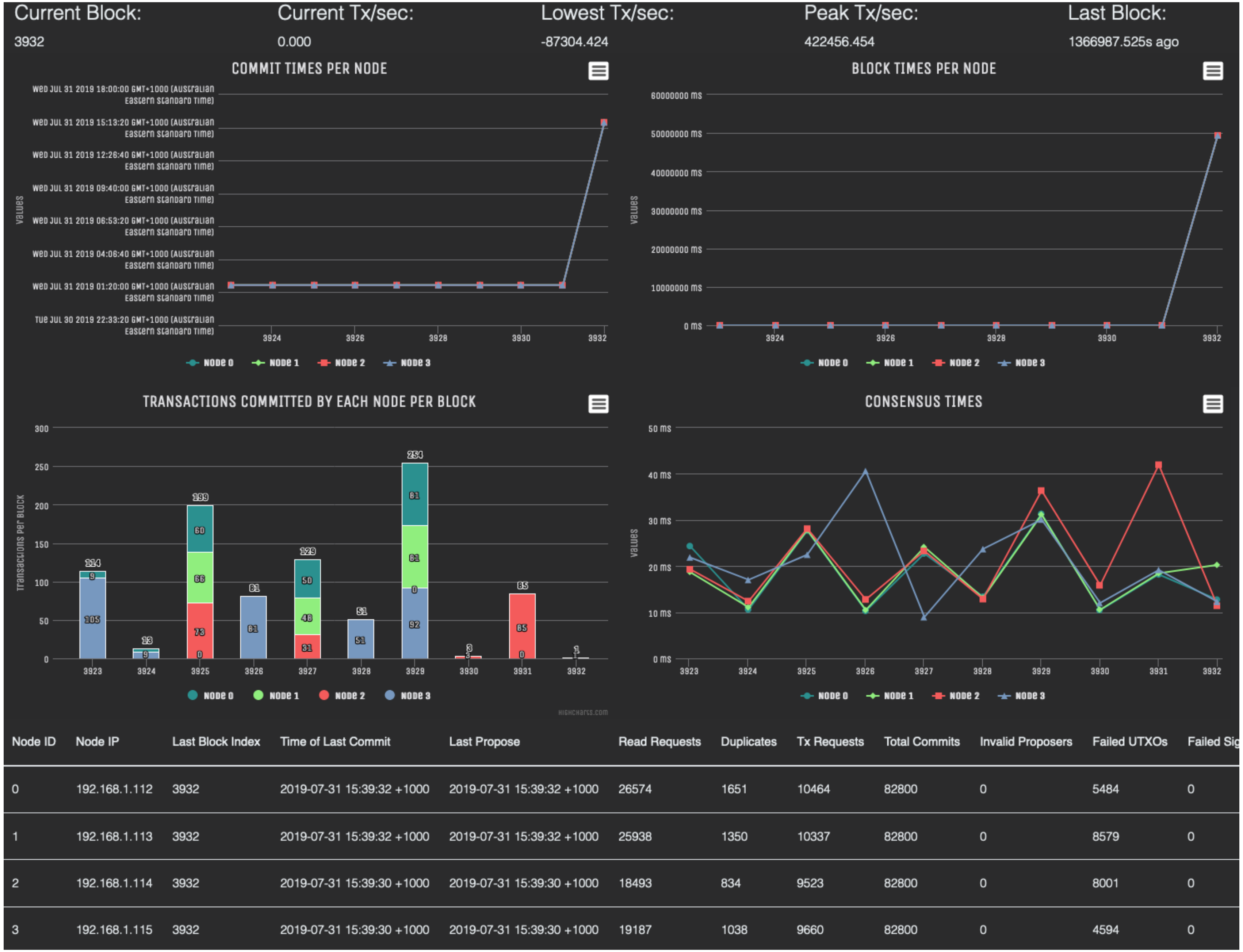
- ~3 years
- 100,000+ LOC
- 10 developers
- 6 programming languages

Components

- Explorer (dashboard)
- Parser (explore blocks)
- Java client
- Dart client
- C# client
- State Machine Replication
- Consensus
- Network



Dashboard



Byzantine Fault Tolerance

- Consensus is deterministic
- Forks are impossible even in infinite executions
- Proof of correctness (cf. p.30-39 of https://arxiv.org/pdf/1702.03068.pdf)
- Formally verified with model checking

Joint Venture

Block8

- 2021 - Block8 is a blockchain service company at the time
- The business grows slowly
- Bull market: many contracts
- Bear market: few contracts
- Product company would allow the business to grow better

Joint Venture

CSIRO accepts to sell most of the IP.

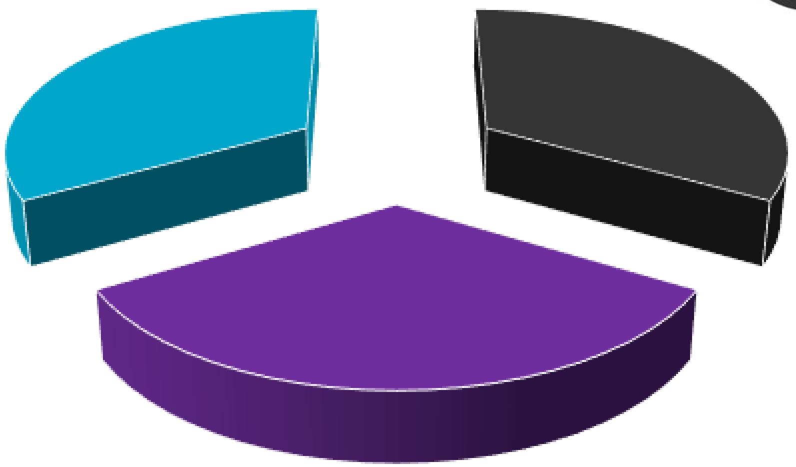
Joint Venture

REDBELLY

CSIRO

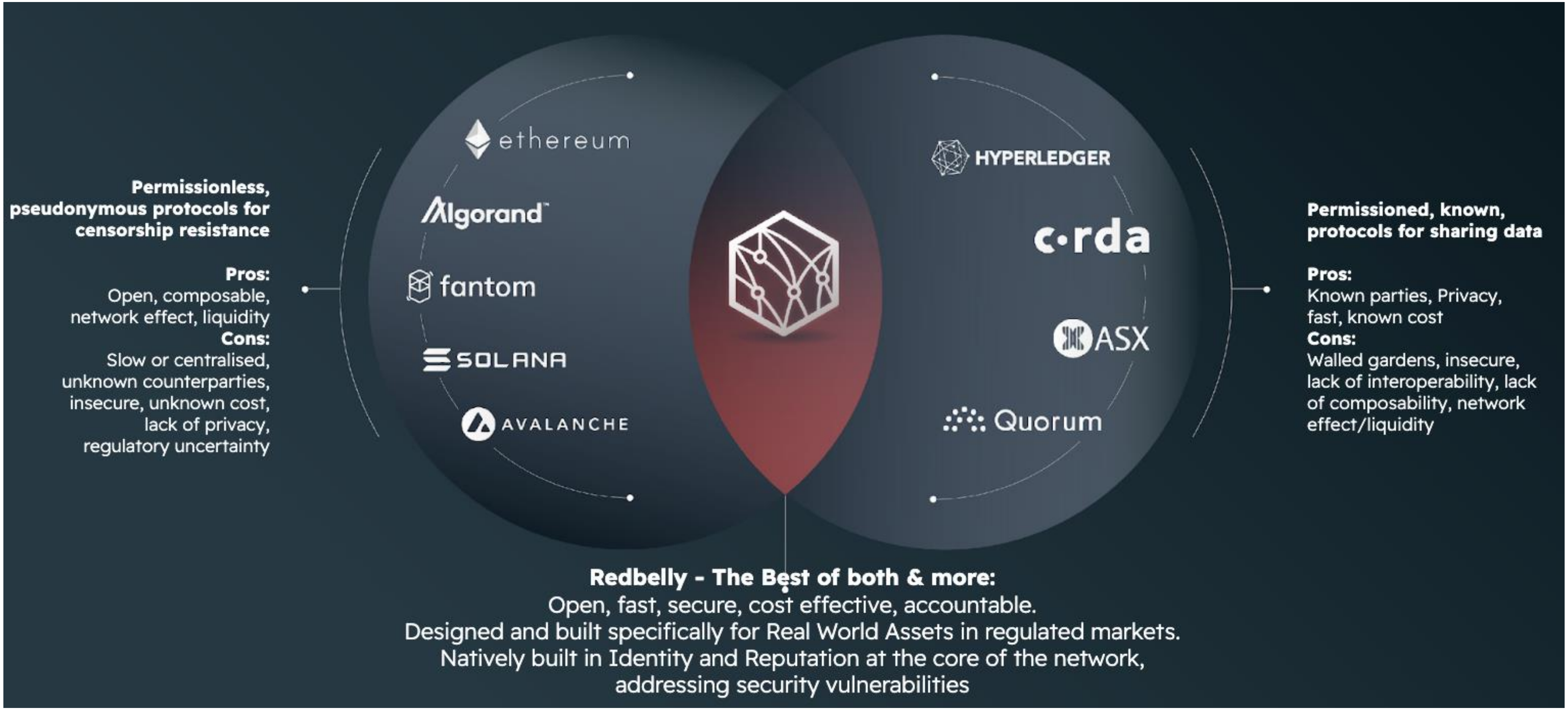
DATA 61

THE UNIVERSITY OF SYDNEY



BLOCK

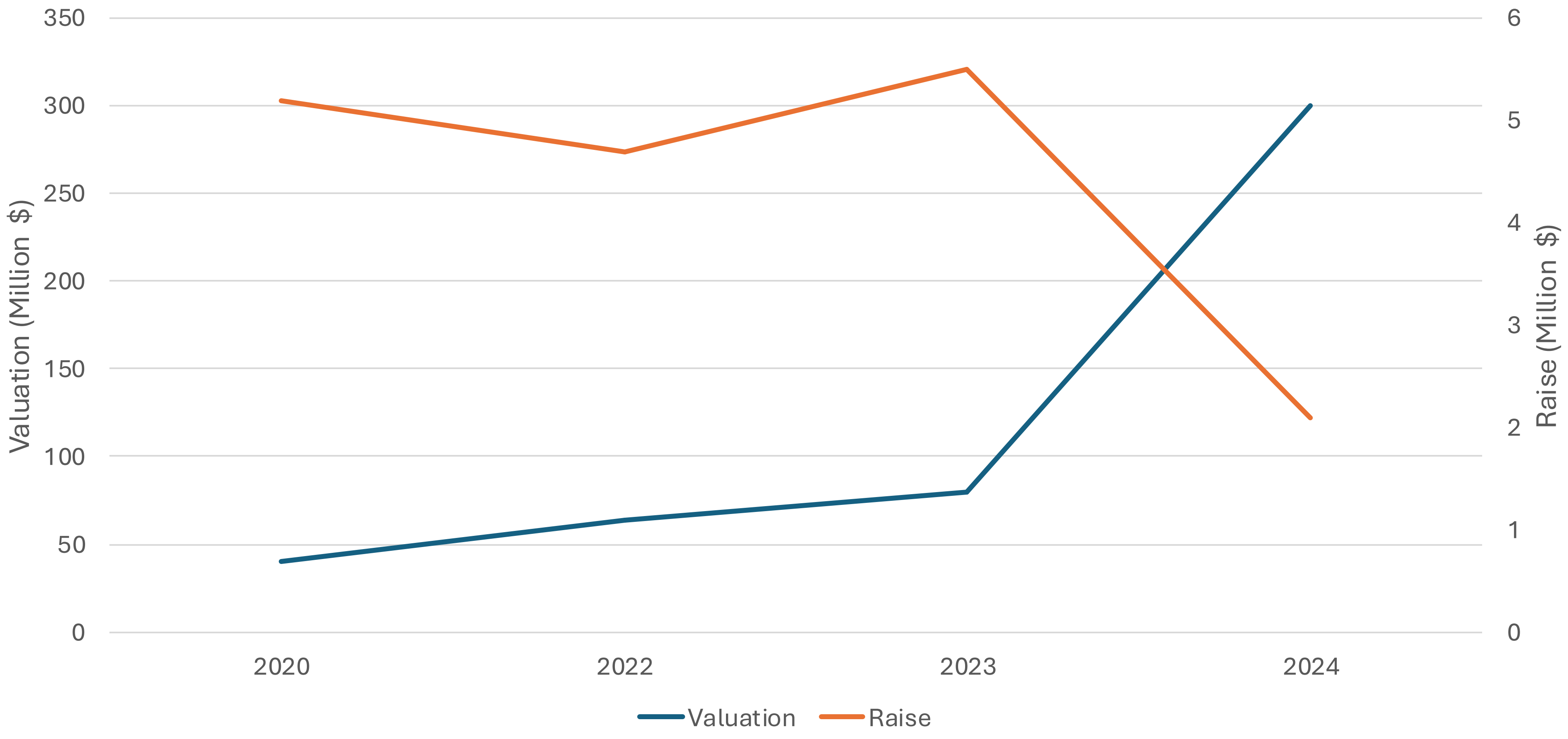
Key Value Proposition



Investors (2024)

THE UNIVERSITY OF SYDNEY
CSIRO
BLOCK 8
BEACHHEAD VENTURE CAPITAL
COGITENT VENTURES
pragma
BRILLIANCE 3.0
CRYPTOPIA
SOLRDAO
CELESTIAL VENTURES
VENTURES
JellyC
FISH DAO
BLACK DRAGON
DUTCH CRYPTO INVESTORS
CSPDAO
aza GROUPS

Investment Rounds (before launch)



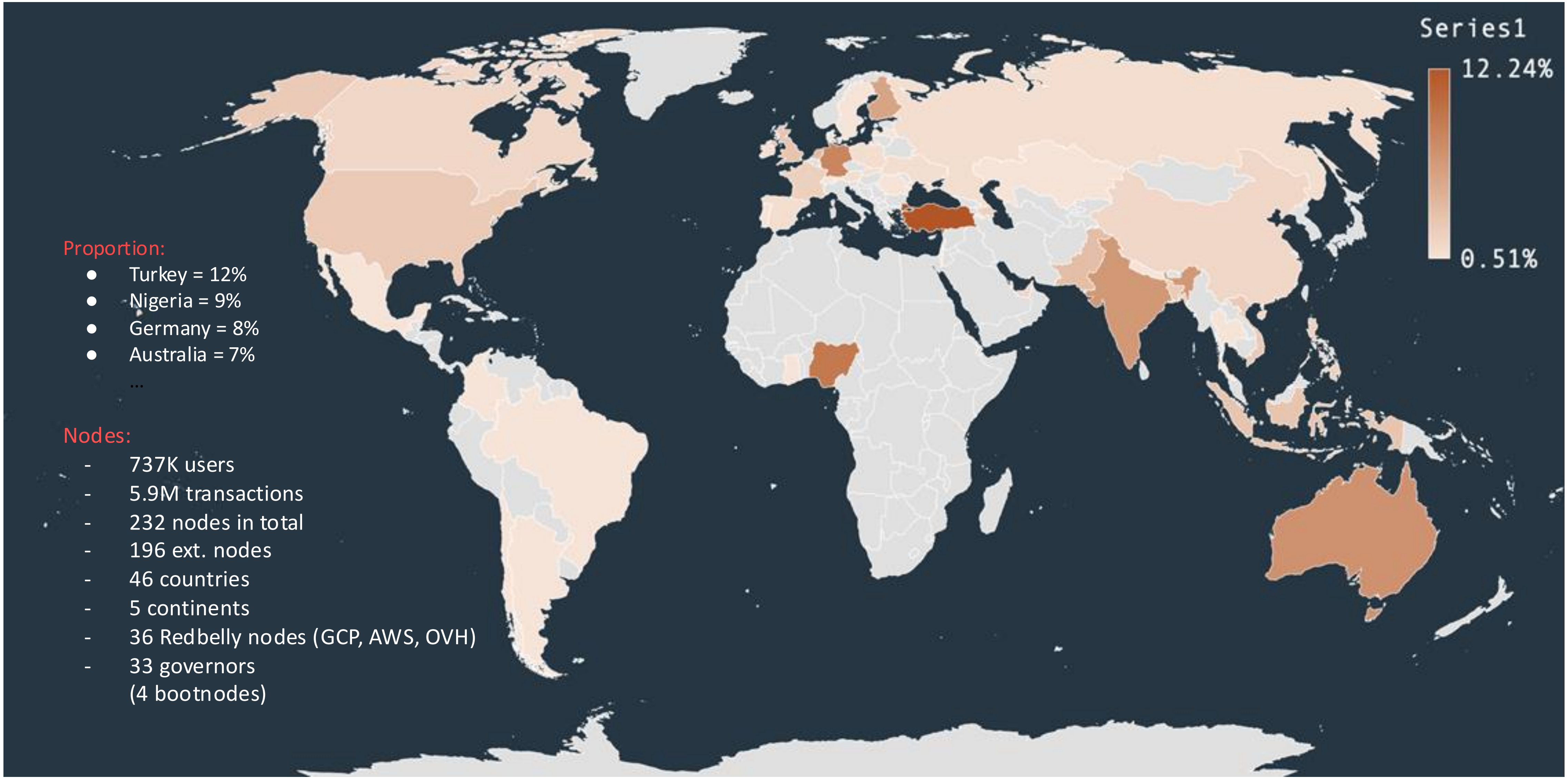
Convincing the Central Bank

Convincing the Central Bank

- 2020 - RBA opens a lab
- Discussion between Vincent and RBA
- Vincent proposes to backup the New Payment Platform
- RBA is very slow at deciding
- 2024 – Redbelly participate in a call for pilot organized by the RBA
- 2025 – Redbelly win the call

In Production

Redbelly Network in Production Today



Proportion:

- Turkey = 12%
- Nigeria = 9%
- Germany = 8%
- Australia = 7%

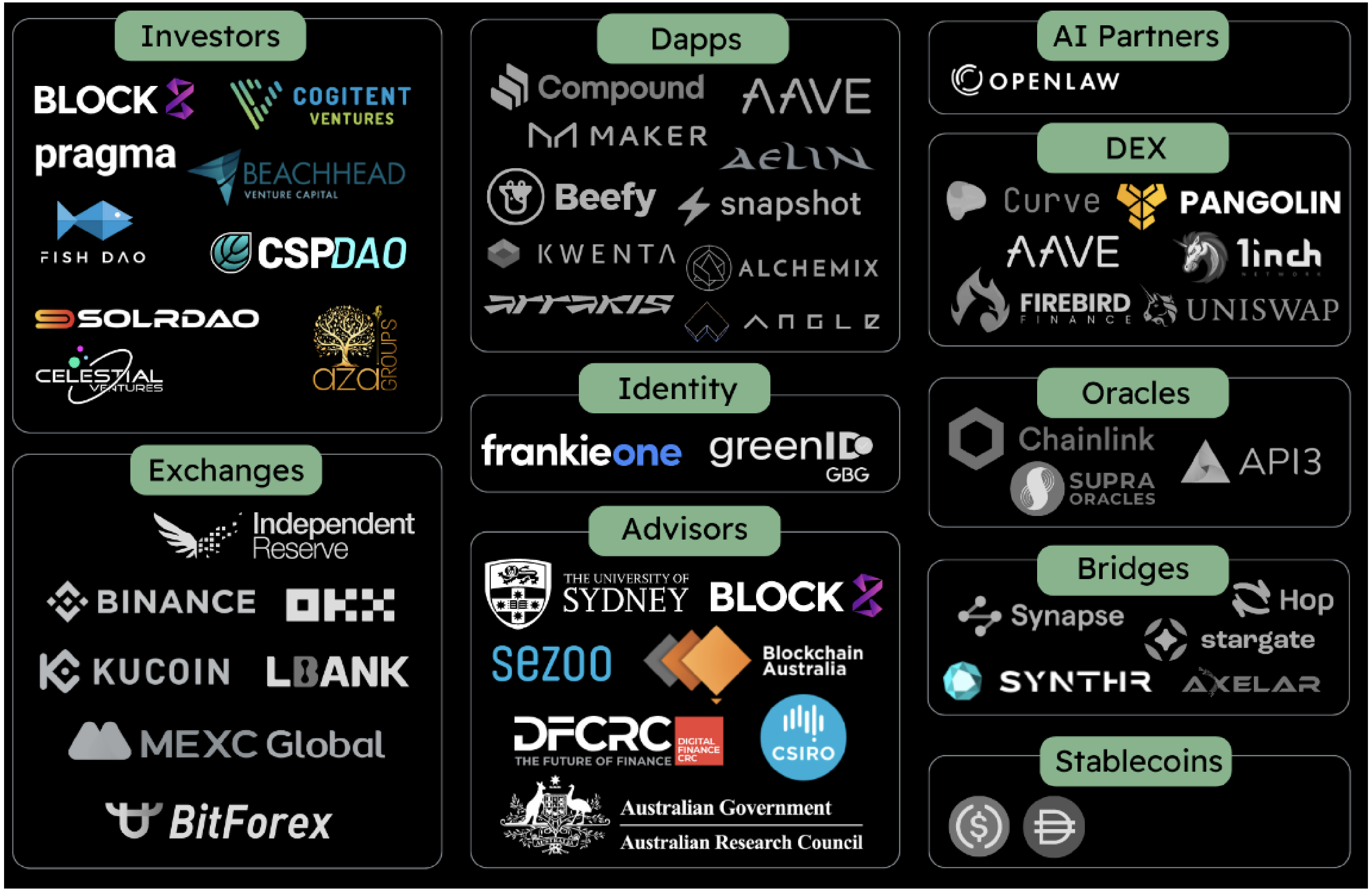
…

Nodes:

- 737K users
- 5.9M transactions
- 232 nodes in total
- 196 ext. nodes
- 46 countries
- 5 continents
- 36 Redbelly nodes (GCP, AWS, OVH)
- 33 governors
  (4 bootnodes)

Partnerships

Ecosystem (2023)



Partnership

Google

REDBELLY

REDBELLY

Convergence of Regulated Agentic AI and Blockchain

Vincent Gramoli - Founder & CTO

© 2024 Redbelly Network Pty Ltd. All rights reserved. Confidential: do not duplicate or distribute without written permission from Redbelly Network Pty Ltd.

Backup

Investment Rounds (before launch)

Category	Year of Raise	Supply (billion)	Supply (%)	Price	FDV	Assets committed on chain	USD Equivalent (million)	Listing unlock %	Lock-up Cliff	Vesting
Seed	2020	1.3	13%	$0.004	$40m	$0	$5.2m	0	6 months	32 months
Private Sale A	2022	0.73	7.3%	$0.0064	$64m	$0	$4.7m	0	2 months	12 months
Private Sale B	2023	0.69	6.9%	$0.008	$80m	$2.5b	$5.5m	0	2 months	10 months
Private Sale C	2024	0.07	0.7%	$0.030	$300m	$83.8b	$2.1m	10%	2 months	8 months
Team		1.0	10%					0	12 months	24 months
USYD & CSIRO		0.2	2%					0	6 months	30 months
Governance DAO		0.3	3%					33%	1 month	35 months
Ecosystem & Community		3.71	37.1%					0	As earned	As earned
Reserve		2.0	20%					0	-	-
TOTAL		10 billion	100%							

*Includes ~18M tokens (or 0.018% of supply) allocated for Marketing Partnerships
^As earned or unlocked from achieving Milestones