

► PATENT PENDING

Blockchain Technology to Settle US Equities

1. Use case
2. Technology
3. Consortium terms

Use Case

2

- ▶ Prime Directive: Do not disrupt existing Wall Street relationships or work flows
- ▶ To DTC or not to DTC?
- ▶ Thread a blockchain through existing architecture in parallel
- ▶ Solve for counter party risk (reconciliation and settlement costs)
- ▶ 5 Pillar consortium Proof of Concept (PoC)

Use Case, participant roles

- ▶ **Domus** - custodian bank and DTC participant
 - Offer services to custodians
- ▶ **Custodian** services IM
 - IM instructs custodian to move assets to Domus' account at DTC: FBO, fully disclosed
 - Domus onramps assets to blockchain, and allocates to custodian, who allocates to IM
- ▶ **Investment Manager** installs a Domus app on order entry software which will
 - Lock asset on side chain (prevent double spend)
 - Domus FIX tag, enter cryptographic signature and hash of legal contract

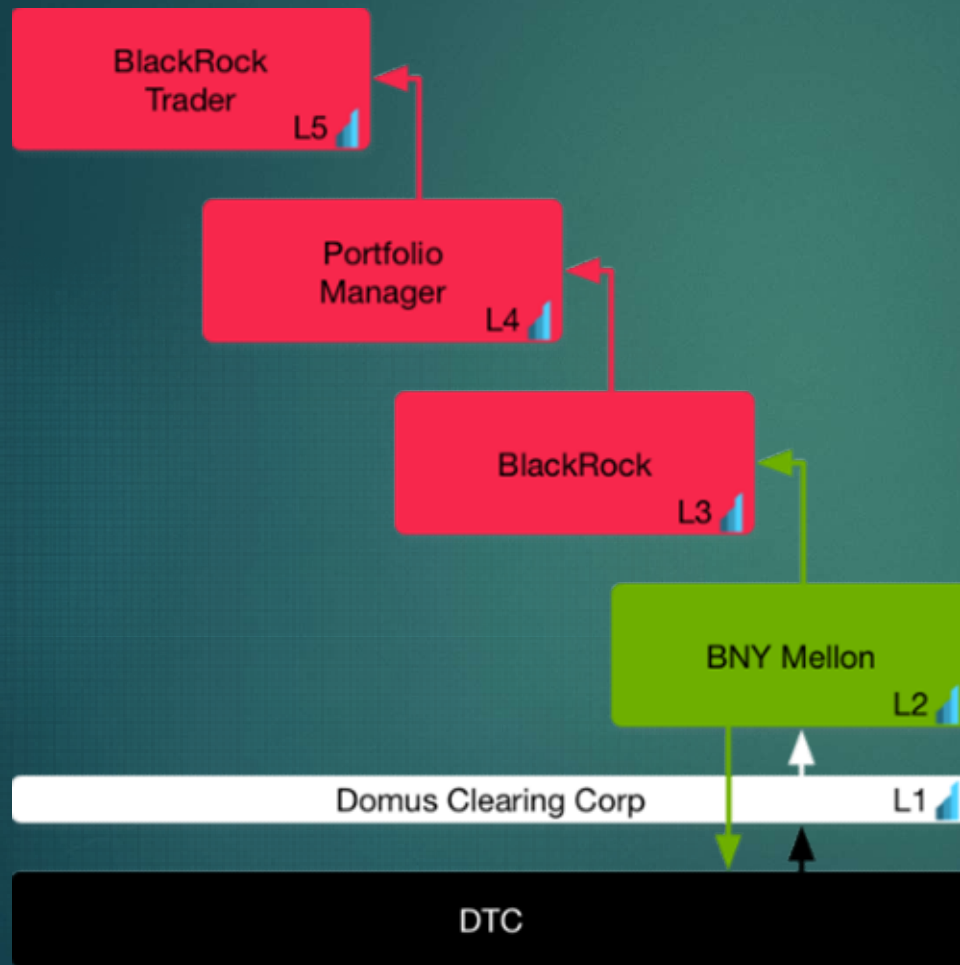
Use Case, participant roles

- ▶ **Broker Dealer** receive orders
 - Recognize Domus FIX tag, cryptographically sign and route to exchange
- ▶ **Exchange**
 - Recognize Domus FIX tags, send the Trade Report to Domus
- ▶ **Domus** ingests trade reports at millions tps
 - Holds assets for several custodians, allowing Domus to internalize settlement
 - Use Smart Contract to settle in T+2
 - Domus sends end of day batch files to DTC, just like every other DTC participant

Use Case, To DTC!

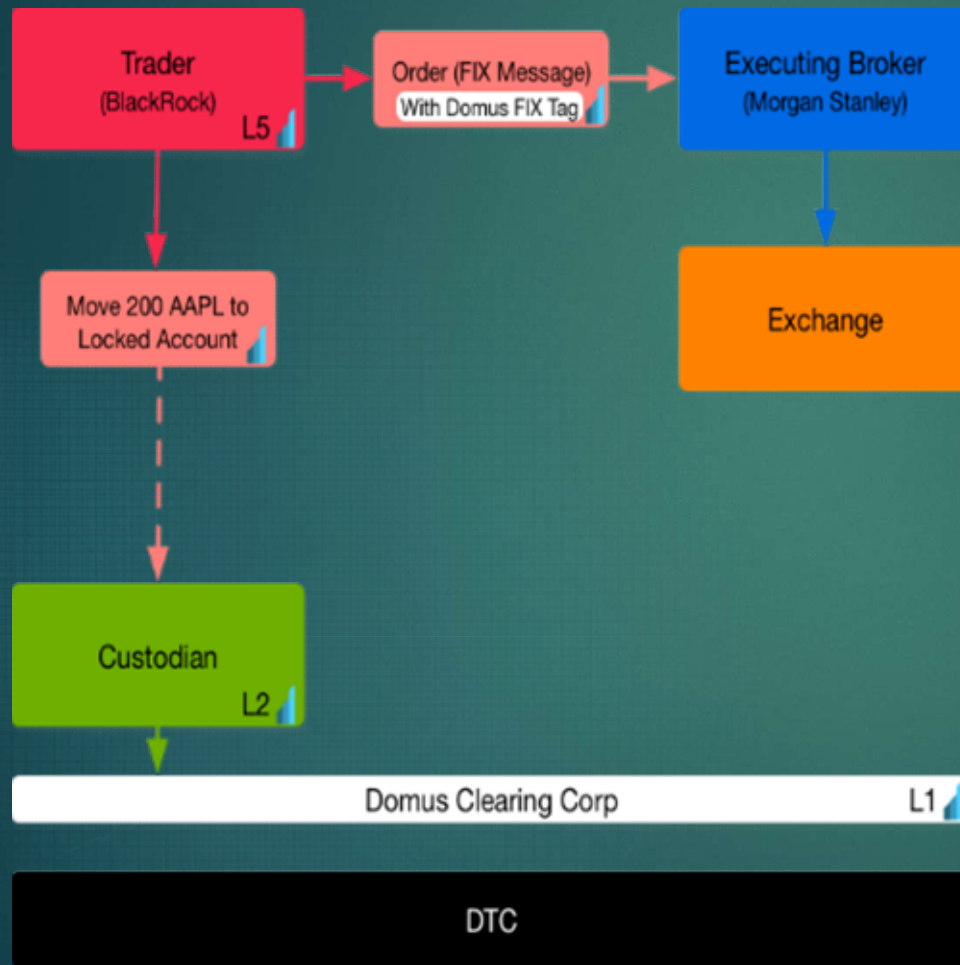
- ▶ **DTCC** services custodians as they do now
 - Domus accounts at DTC are FBO the custodians and fully disclosed so DTC can service assets
 - Domus is a thin software layer between DTC and custodians, a “master custodian”

Use Case, Custodian



- ▶ L1 is the main blockchain, an immutable, append only data base
 - IM's instruct Custodians to transfer 'some' assets from their DTC account to Domus' DTC account
 - Domus propagates data and permissions to Custodians on L2
 - Custodians propagate data and permissions to their customers, up to L5`

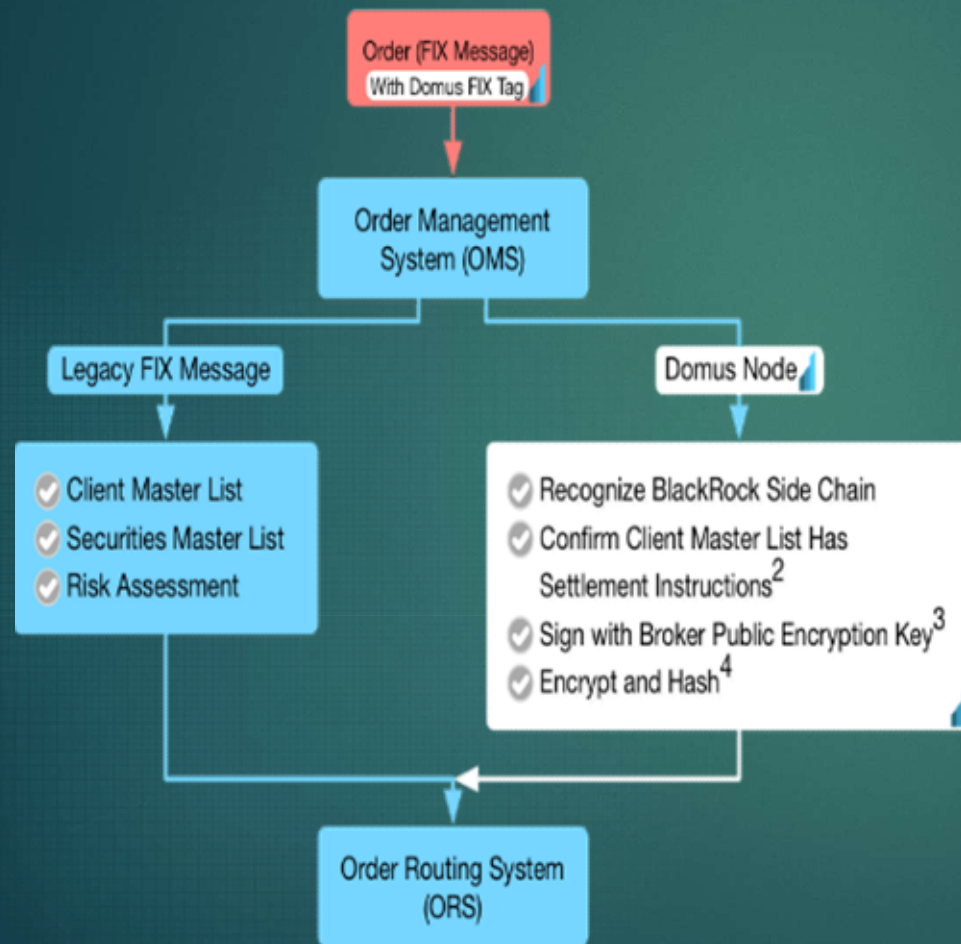
Use Case, IM



► Trader enters order which:

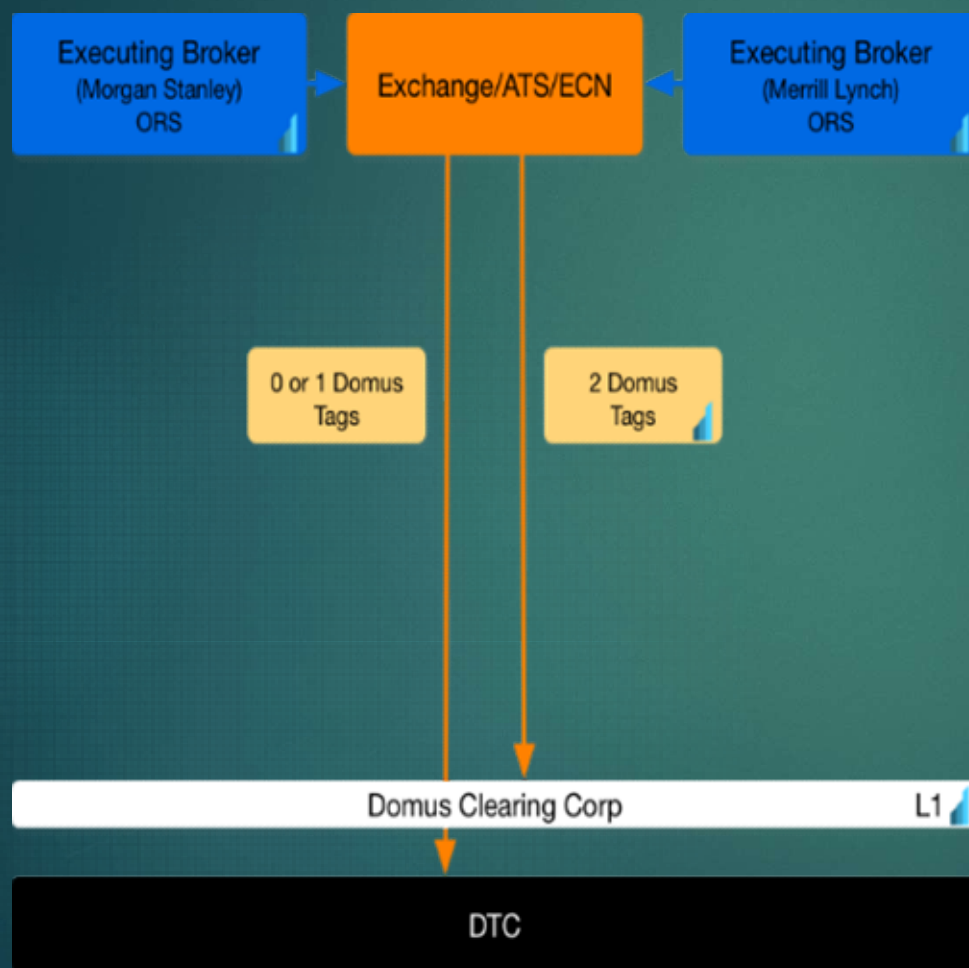
- Locks funding asset on L5 and propagates that back to L1
- Cryptographically signs order
- The Domus FIX tag is constructed into the FIX message and sent to the Broker Dealer

Use Case, Broker Dealer



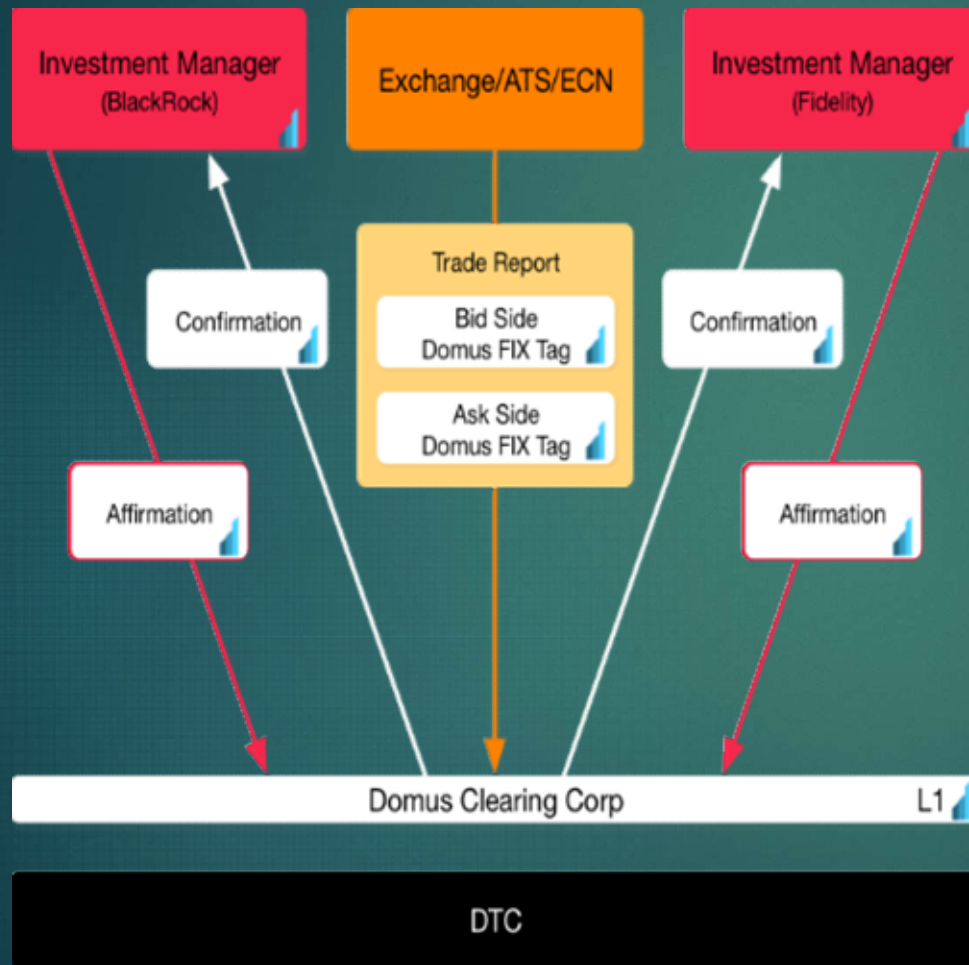
- ▶ BD Order Management System (OMS) recognizes the Domus FIX tag
 - OMS sends Domus FIX tag to a new HSM called the Domus Node
 - The Domus Node checks settlement instructions
 - The BD cryptographically signs the Domus FIX tag
 - Domus tag is hashed to reduce latency for speed
 - ORS sends order to an Exchange

Use Case, Exchange



- ▶ Exchange receives the order from the BD's ORS
 - If no Domus tags, send order to DTC for T+3
 - If one side has a Domus Tag, send order to DTC for T+3
 - If both sides have Domus tags forward the trade report to Domus

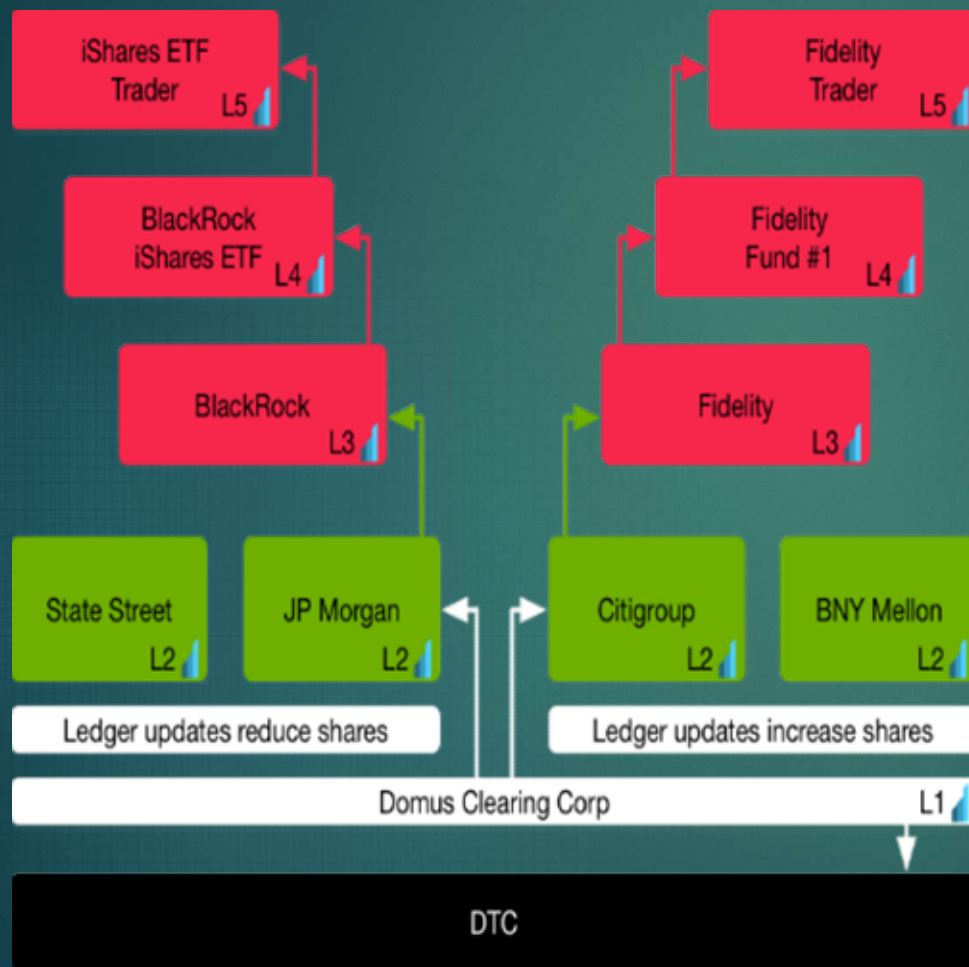
Domus effects STP



► Domus receives trade reports

- Domus uses IM signatures to send confirmations
- IM's compare the confirms to the orders
- IM's affirm trades
- Domus makes STP match
- Software step, does not require FINRA membership

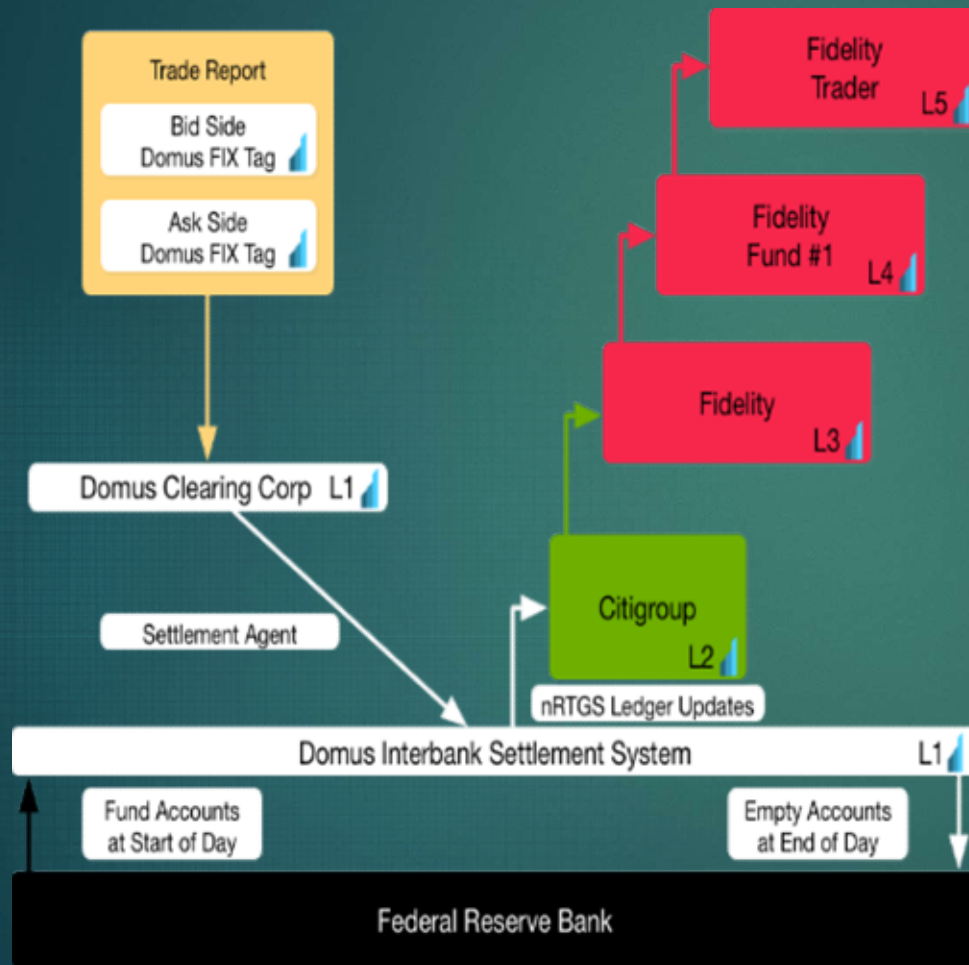
Domus effects settlement



▶ Domus updates the ledgers at custodians moving stock and cash

- Domus updates ledgers at custodians - L2
- Custodians allocate trades to IM's and funds L3-L5
- Traders (L5) can trade again in nRT
- Domus nets and sends batch files to DTC at end of day
- DTC services custodians directly

Domus settles cash side



► Domus creates Domus Interbank Settlement System (DISS), taking best practices from NSS and CHIPS

- Cash is on-ramped and off-ramped to and from the Fed daily, and intraday if necessary
- DISS becomes a "Settlement Agent"
- DISS nets and sends batch files to the Fed daily
- The Fed services custodian banks directly

Technology, The Domus Blockchain

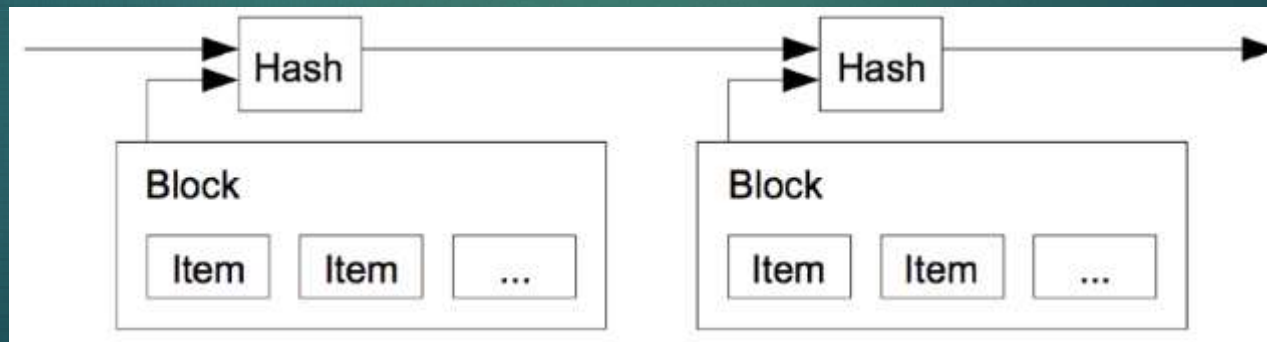
- ▶ Scalable: benchmarked at 1.23 million tps
- ▶ Can be scaled up to 10 million easily
- ▶ Runs on AWS at less than \$50 per hour

Technology, comparing crypto ledgers

	Max Transaction Rate	Tracks Assets and Liabilities?	Trust Model
Bitcoin	~7tps	No	Proof of Work
Ripple	~few thousand tps	Yes	Federated Voting
Domus	10M+ (scalable)	Yes	Trusted

Technology, What is a blockchain?

- ▶ Satoshi described a block of items and a timestamp server where each block contains a hash of the prior block creating a Merkle root, e.g. immutability
- ▶ Data is transmitted using cryptographic digital signatures which are verified before writing to the blockchain
- ▶ GIT is a centralized system based on a Merkle DAG, so GIT is a blockchain where participants pull data – no POW.



Technology, architecture overview

- ▶ Custom Micro Service Framework
- ▶ Stream Processing (low latency)
- ▶ Micro Batching (higher latency, higher throughput)

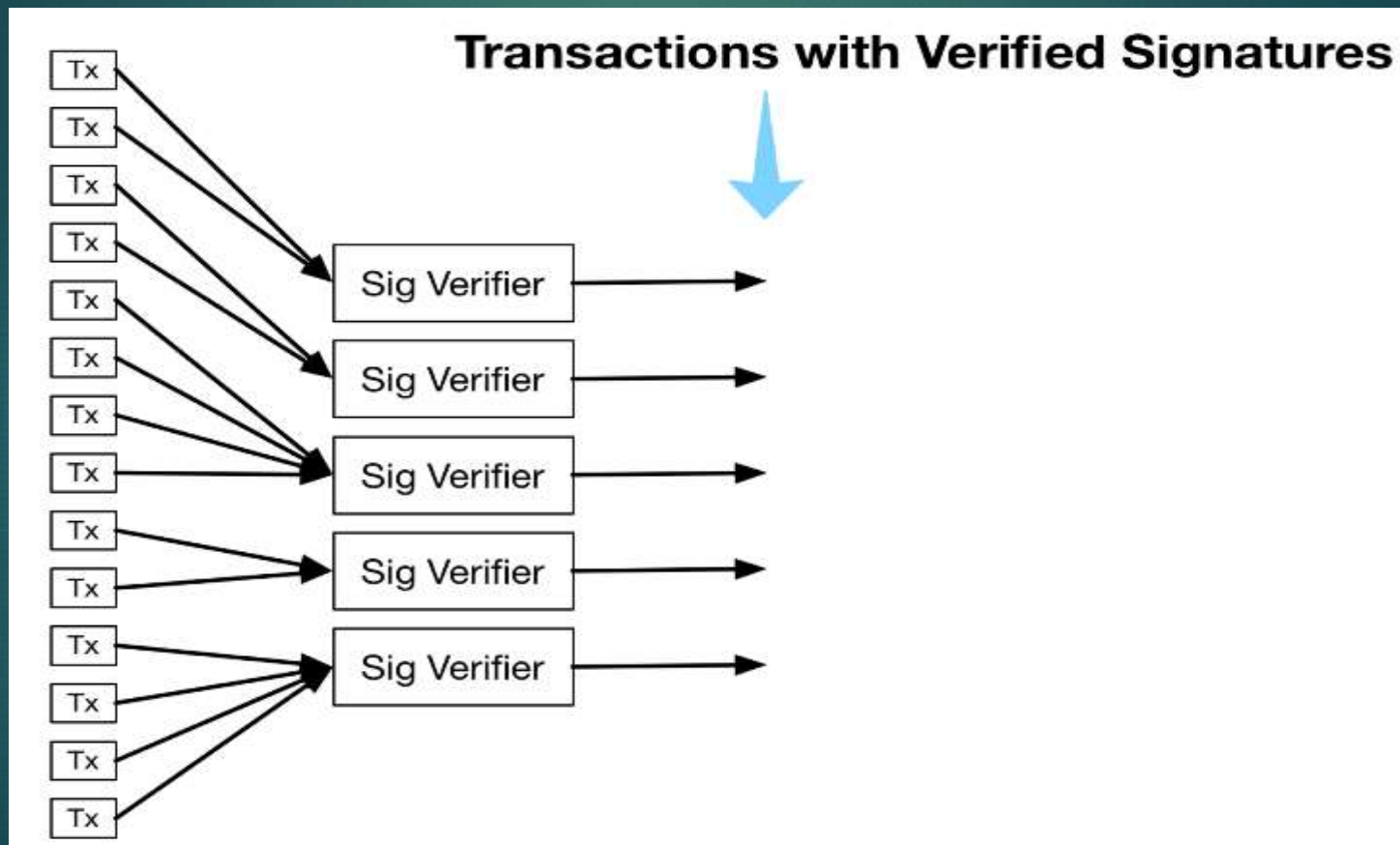
Technology, architecture components

- ▶ Signature Verifier
- ▶ Transaction Batcher
- ▶ Block Maker
- ▶ Client

Technology, Signature Verification

- ▶ Computationally expensive
- ▶ **But** problem is embarrassingly parallel
- ▶ We choose ed25519 signatures for high speed and high security
- ▶ Verified signatures are passed to transaction batching

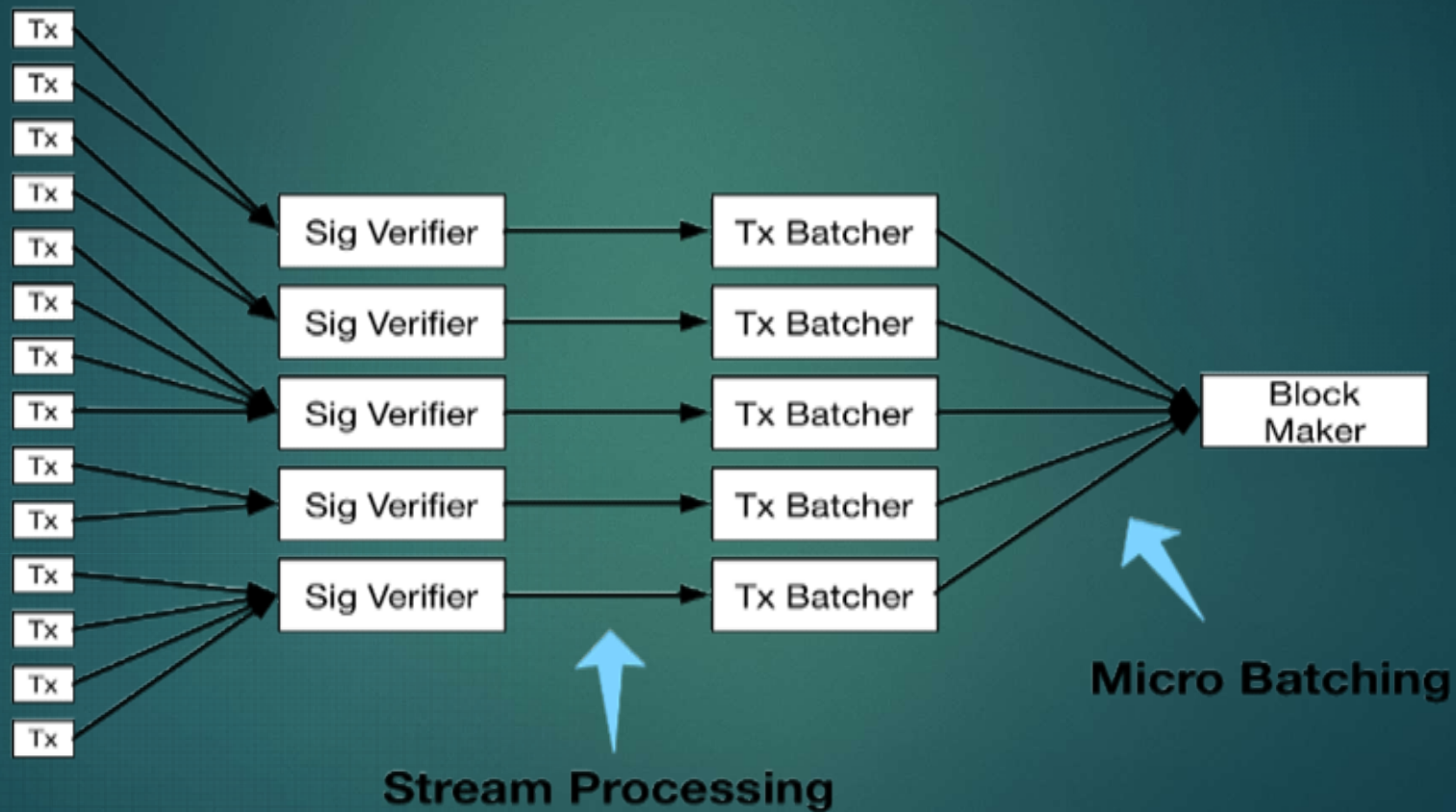
Technology, Signature Verification



Technology, Transaction Batching

- ▶ Run any batch operation logic (net balance changes)
- ▶ Currently set for 10,000 transactions over socket stream, but can be set by X transactions, or Y milliseconds.
- ▶ Compress as one file using gzip
- ▶ Each message has 10,000 transactions and is uploaded as an http file.
- ▶ gzip file is sent to block maker

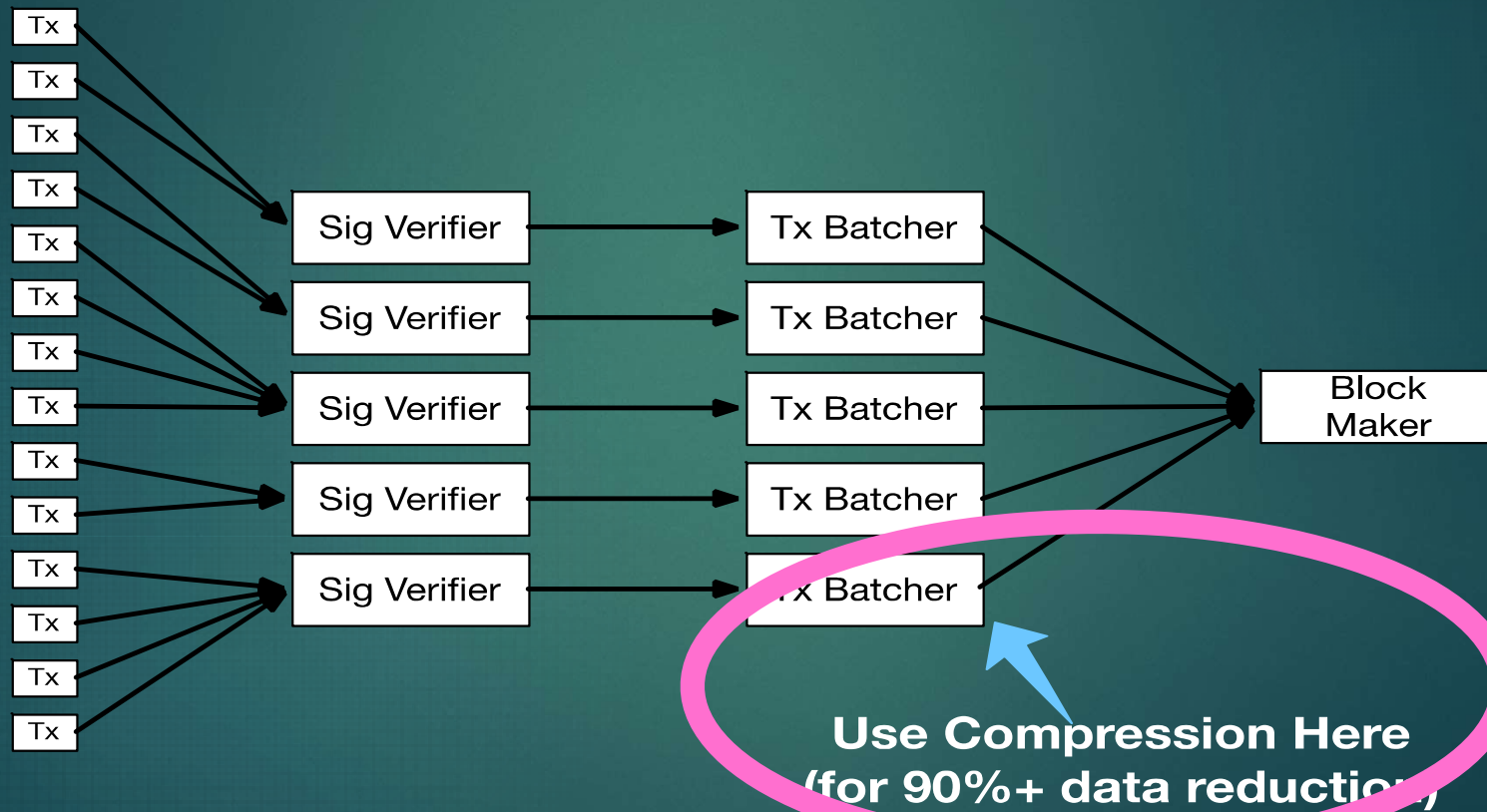
Technology, Transaction Batching



Technology, Block Maker

- ▶ In-Memory Key-Value Store (Redis)
- ▶ Persistence via fsync, one per second
- ▶ One block per second
- ▶ Key for each second points to linked-List of transactions for that second
- ▶ Separate process computes Merkle Roots for blocks

Technology, Data Storage Solution



Technology, Benchmarks

- ▶ Setup: 26-Servers
- ▶ 1x block maker & Redis Server (where the blockchain is stored)
- ▶ 25x TX Batchers, Signature Verifier, Client
- ▶ Max TX Size: 256-Bytes
- ▶ Total Ingest: 1,240,000 tps
- ▶ We are CPU limited on Signature Verifiers

Accounting, Single-Entry

Bitcoin Example

Date	From	To	Amount
March 1	Block Reward	A	25 BTC
March 1	A	B	5 BTC
March 1	B	C	2 BTC

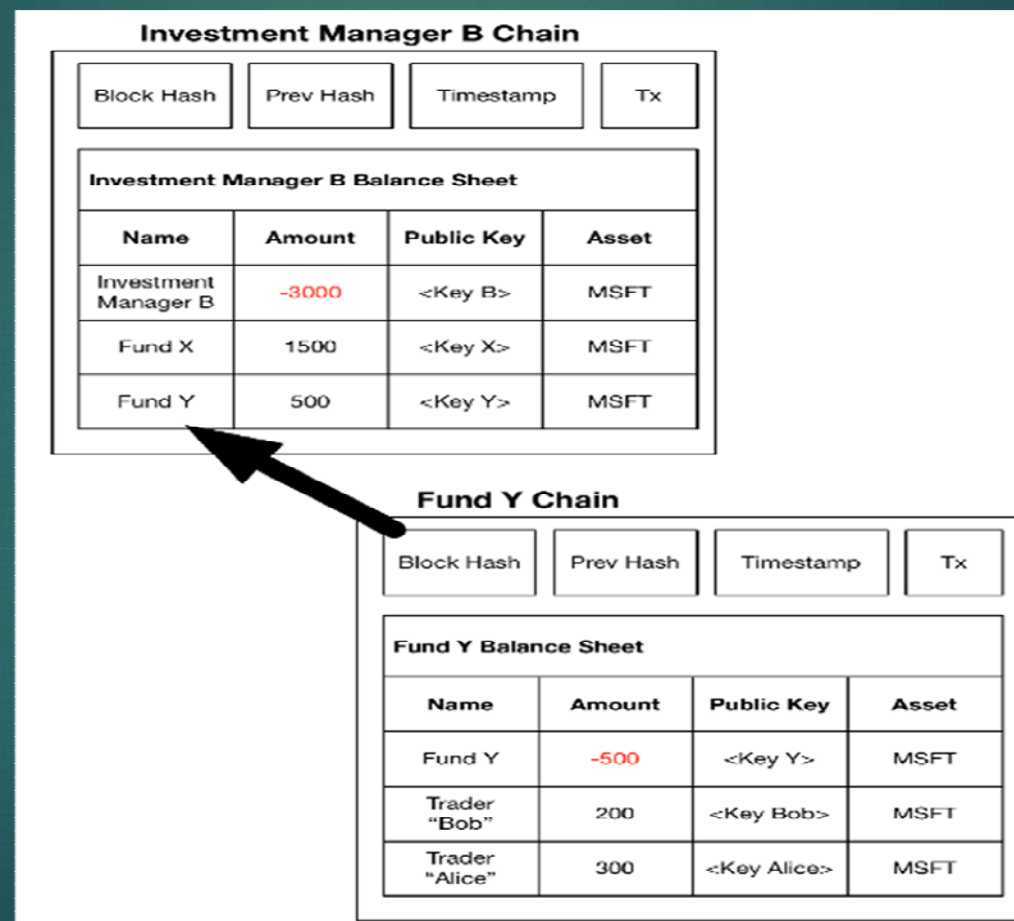
Accounting, Double-Entry

26

Domus Example

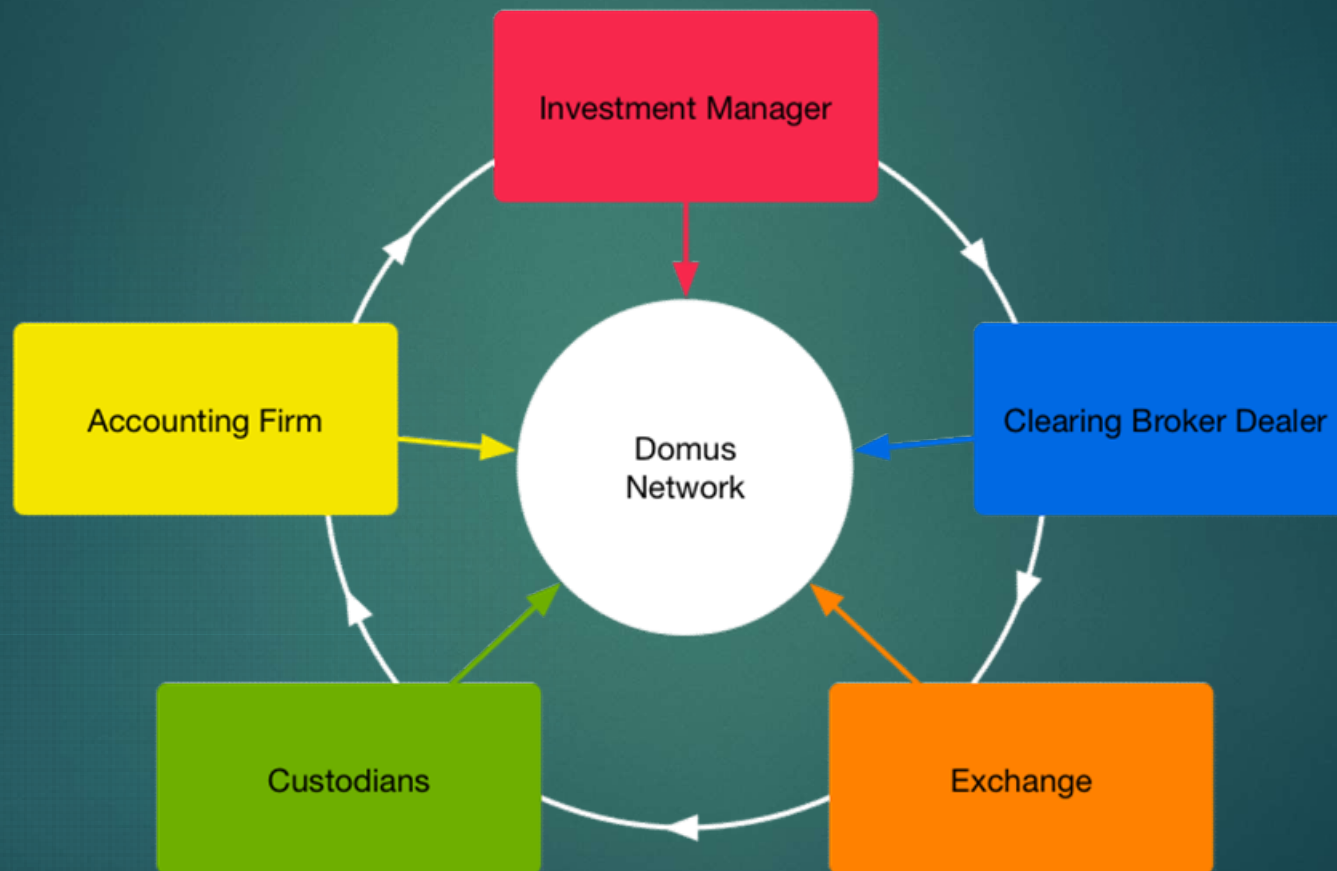
Date	Account	Debits	Credits	Balance
March 1	A		+100 MSFT	+100 MSFT
March 1	C	-100 MSFT		-100 MSFT
March 1	B		+300 MSFT	+300 MSFT
March 1	C	- 300 MSFT		-400 MSFT

Accounting, linked Domus side chains



Consortium, Five Pillars

28



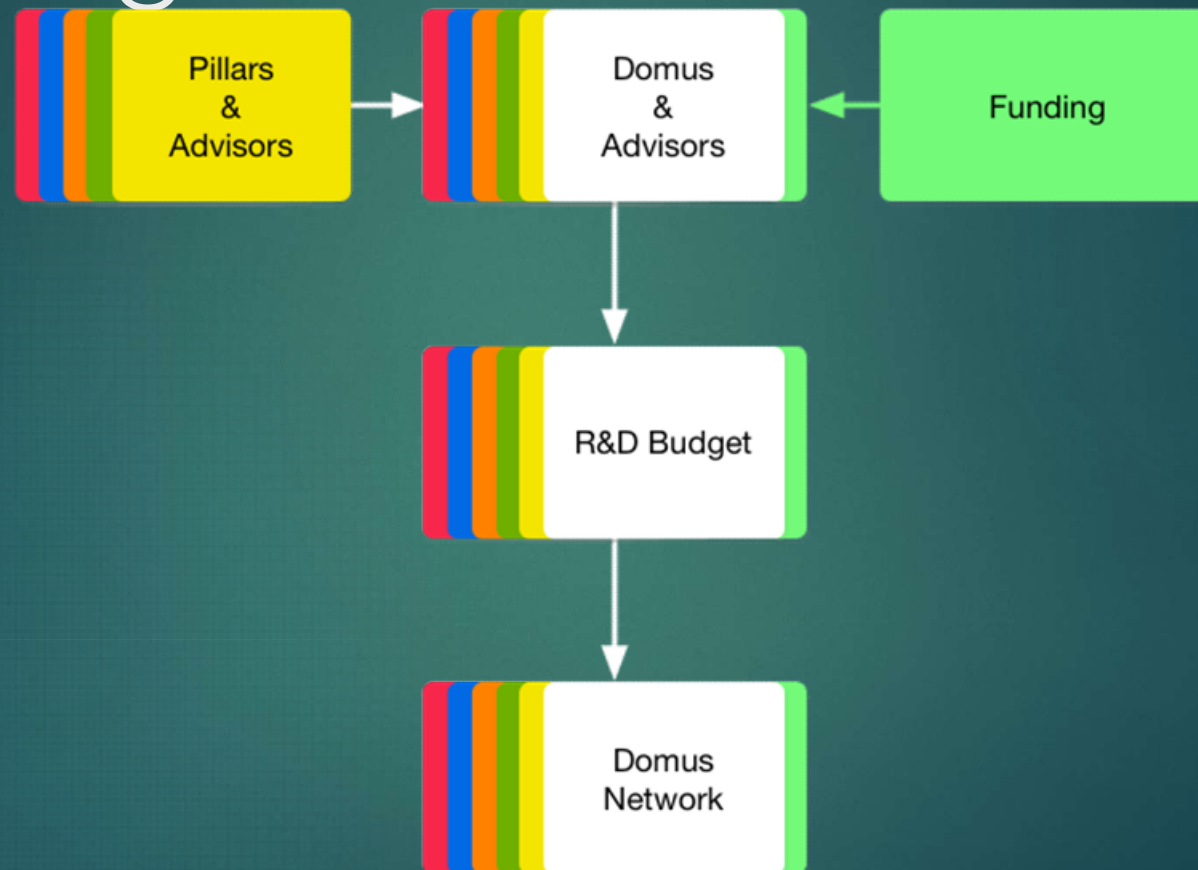
Consortium Terms, 2 year Proof of concept

- ▶ Big 4
 - ▶ Statement of Work
 - ▶ co-ordinates Pillar meetings, work flows and problem solving
 - ▶ Installs software in confidential test environment
 - ▶ Compliance, re-papering and regulatory issues
- ▶ Cash: Domus pays you, underwriting your IT budget
- ▶ Equity: You earn equity in Domus common stock
- ▶ Pillars allocate resources to work with Big 4
- ▶ Exclusive: Only one Pillar from each industry sector
- ▶ Non –Exclusive: You are free to work with others

Consortium, Benefits and Expectations

- ▶ Benefits
 - ▶ Shape to new Wall Street settlement system with your vision, rather than someone else's vision
 - ▶ Use equities implementation to inspire other use cases across your firm.
 - ▶ First mover advantages, product development
- ▶ Expectations
 - ▶ Dedicated personnel, access to systems
 - ▶ Participation in strategy and problem solving

Business Plan, Funding Model



Business Plan, Financial highlights

- ▶ Budget \$25M

▶ Statement of Work	\$5M
▶ Custodian Bank allocation	\$4M
▶ IM, BD and Exchange allocation	\$6M
▶ Core Blockchain development	\$3M
▶ Compliance legal	\$3M
▶ Corporate overheads	\$4M

Business Plan, Objectives

- ▶ Receive draft Statements of Works from Big 4
- ▶ Close 5 Pillar consortium
- ▶ Close \$25M A Round
- ▶ Start two year Proof of concept work
- ▶ Offer commercial product to the industry
- ▶ Generate network effect

Business Plan, Revenue and profit

- ▶ Settlement Costs
 - ▶ Domus charges custodians, and custodians service IM's, marking up fee
- ▶ Counterparty Risk
 - ▶ Balance Sheet requirements at BD's and costs are accurately measureable
 - ▶ Domus can charge BD's for ability to reduce their cost of capital
 - ▶ BD's benefit from lower settlement and capital costs, becoming more competitive

Team

35



Joe Forster: Chairman & CEO

Founder/Owner-Operator of Fortrend Securities Inc since 1992, member FINRA, registered with the SEC.

Joe is also a representative of PCG Equity, a private investment company with in excess of \$1.5 billion of assets.

Previously Joe worked in research at Smith Barney in New York and as an investment banker at Merrill Lynch.



Kevin Woods: Director, in house counsel

Litigated cases in federal and state courts and in various arbitration forums, including FINRA, AAA, and JAMS. Focus on securities litigation, securities enforcement defence before the SEC, Department of Justice, FINRA.

Prior to co-founding White & Woods, Kevin was senior counsel at Bingham McCutchen LLP, where he was an active member of its Broker-Dealer Group. Kevin served for five years as an assistant district attorney in the Manhattan District Attorney's Office.

Team

36



Roy Epstein: CFO

Roy is a principal at PCG Equity an investment firm with more than \$1.5 billion of assets. Before that he was a Managing Director at JP Morgan Chase in the investment banking group.

Mr. Epstein began his career at Arthur Andersen & Company in 1985 and is a Certified Public Accountant. Upon graduation from Columbia Law School, he was an attorney at Cravath, Swaine & Moore, in New York.



Arman Pahlavan: Secretary

Arman is counsel for Domus, is a Partner at Perkins Coie's Emerging Companies and Private Equity groups. Arman has represented clients in private equity, venture capital and mergers and acquisitions transactions valued at billions of dollars. He has acted as counsel in the representation of public companies, foreign private issuers and in securities litigation.

Team

37



Rhett Creighton: CTO

Rhett Creighton has a Master's in Engineering from MIT. He's spent the last 12 years building secure and scalable internet applications for a variety of industries including nuclear power, cloud-hosted operating systems and consumer finance.