CAS Round Table: Blockchain and Self-Sovereign Identity

Stephen J. Mildenhall

November 2018

ST. JOHN'S UNIVERSITY
Tobin College of Business
School of Risk Management

Discussion Topics

1. Bitcoin Mechanics—Not Bitcoin as Money
2. Lightning Network and Collateral
3. Application Flowchart and Insurance Applications
4. Trust and Identity
5. Self-Sovereign Identity
6. Zero Knowledge Proofs

Bitcoin

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

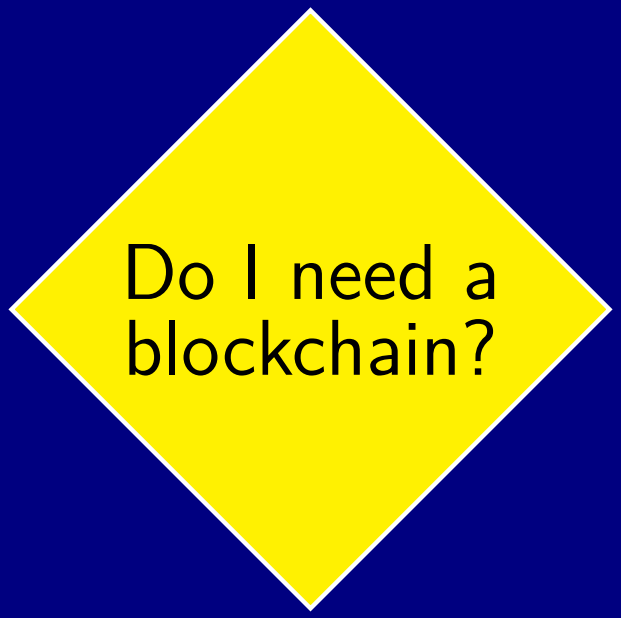
Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto (2008)

Lightning Network and Collateral

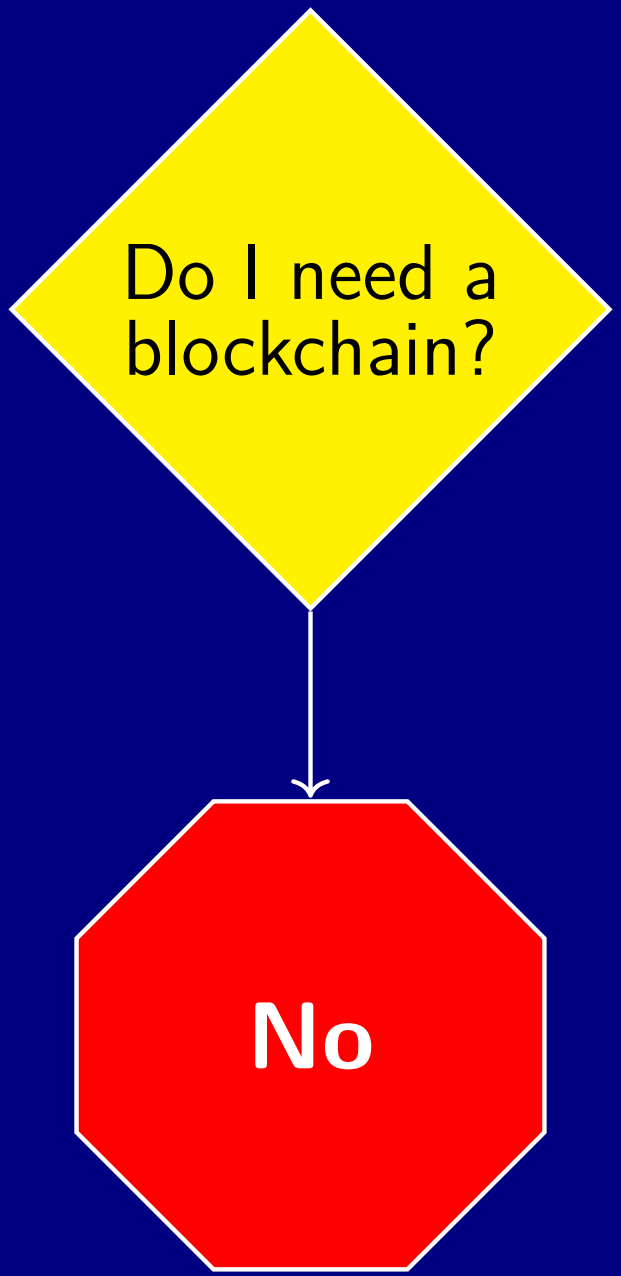
Application Flowchart and Insurance Applications

Birch Model Decision Flowchart

Birch Model Decision Flowchart



Birch Model Decision Flowchart



Capability Refinements Are In Conflict

Between	**and**	there is a **conflict**
Obvious TTP	Blockchain	Trusted third party administers SQL DB
Public	Permissioned	Coordinate without blockchain
Open source	Governance	Uncoordinated open network = forks
Privacy	**Verifiability**	Information needed to verify transactions
Trust	Performance	Low/no trust = poor performance
Access	Efficiency	Guaranteed access, distributed = expensive
PII	Public	Expectation of privacy
PII	Immutable	GDPR Right to be forgotten
Me	Everyone else	**Coordination** or **technology** problem?

Capability Refinements Are In Conflict

Between	**and**	there is a **conflict**
Obvious TTP	Blockchain	Trusted third party administers SQL DB
Public	Permissioned	Coordinate without blockchain
Open source	Governance	Uncoordinated open network = forks
Privacy	**Verifiability**	Information needed to verify transactions
Trust	Performance	Low/no trust = poor performance
Access	Efficiency	Guaranteed access, distributed = expensive
PII	Public	Expectation of privacy
PII	Immutable	GDPR Right to be forgotten
Me	Everyone else	**Coordination** or **technology** problem?

- Confidential transactions can keep the amount and type of assets transferred visible only to participants in the transaction (and those they choose to reveal the blinding key to), while still cryptographically guaranteeing that no more coins can be spent than are available

Blockchain: Finance and Insurance

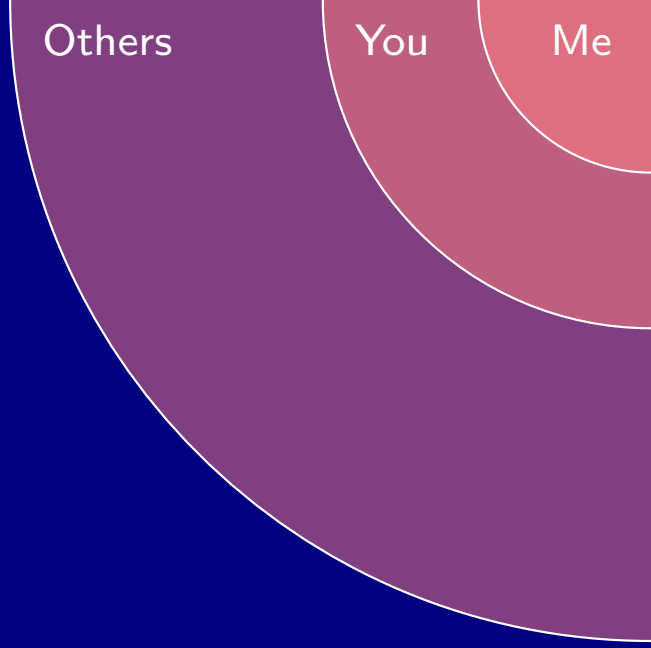
R3 and Corda, Chain; B3i, Blocksure, Etherisc, TeamBrella

- Blockchain incorporating some, but not necessarily all, components of Bitcoin network would enable efficiencies
  - Shared view of truth: not my copy vs. your copy, no reconciliation; hash integrity and validation ensures we all have identical databases
  - Database can be private
  - Validation can involve authorities or decentralized consensus mining
- Effectiveness requires a willingness to change processes and behaviors
  - One party can post a contract and the other signs it to finalize
  - Definitive language available to both parties. . . but they sill have to do the work
- Blockchain: { a good tool to **enable** / won't magically **enforce** } contract certainty

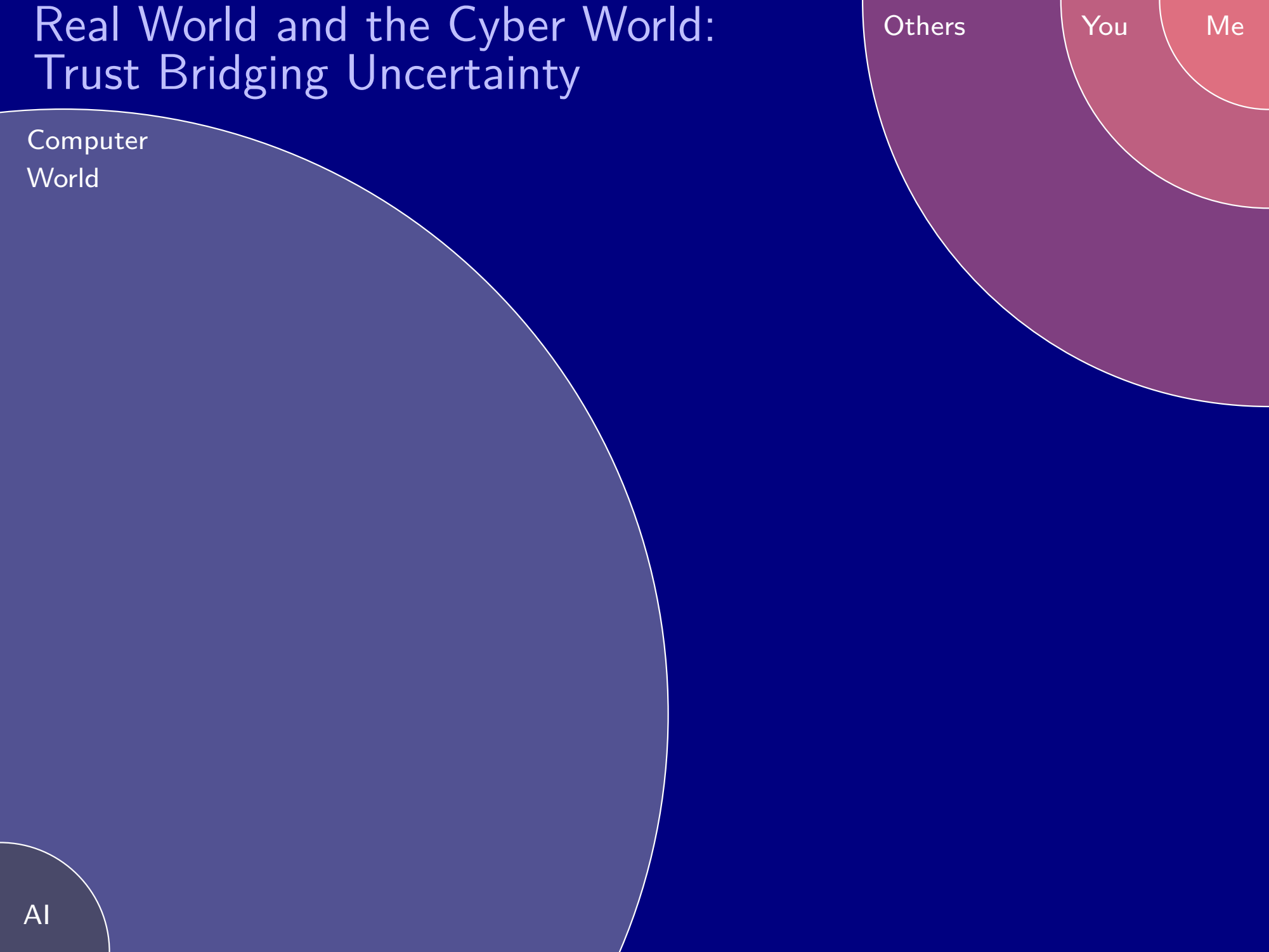
Trust and Identity

Real World and the Cyber World: Trust Bridging Uncertainty

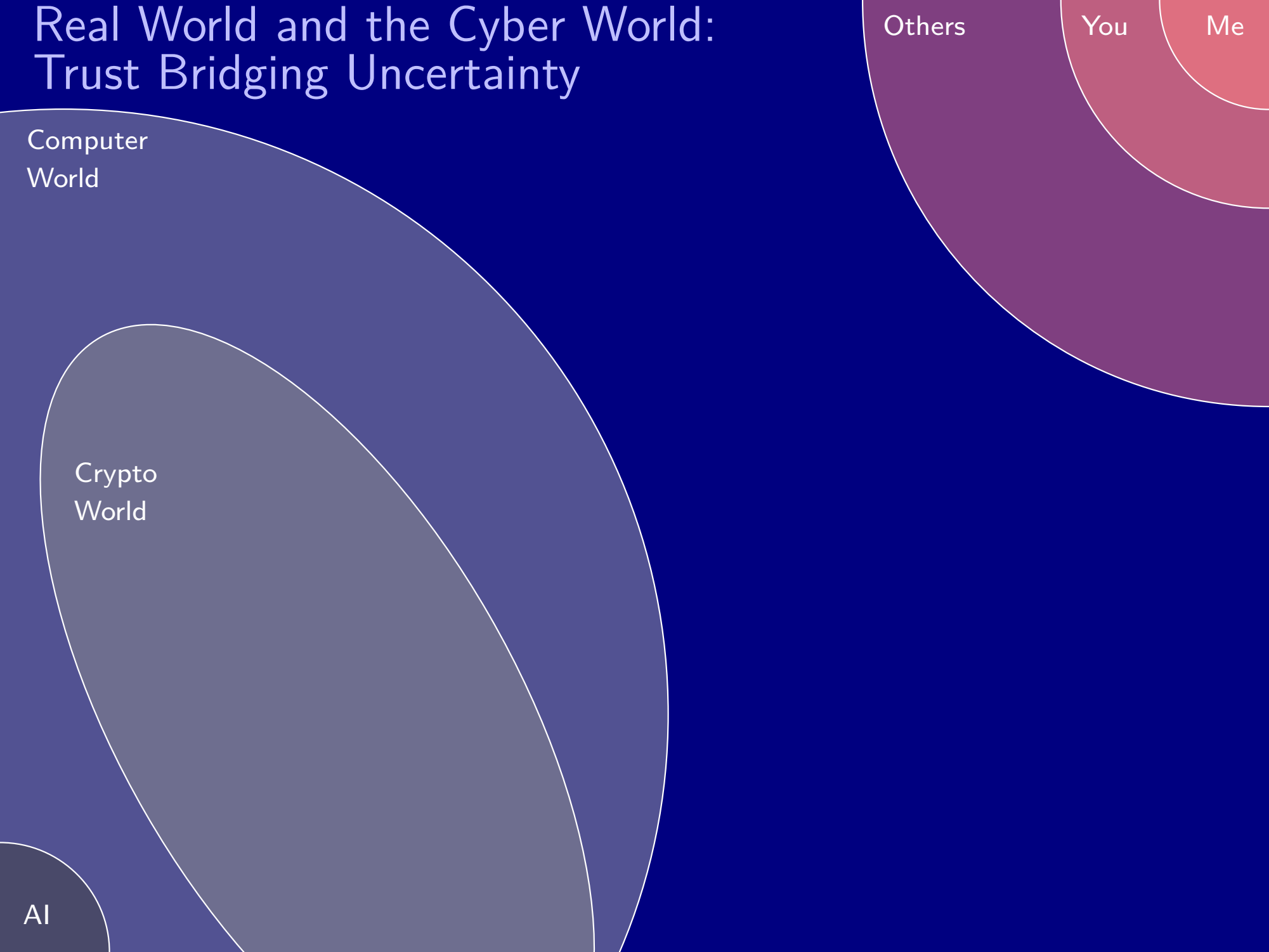
Real World and the Cyber World: Trust Bridging Uncertainty



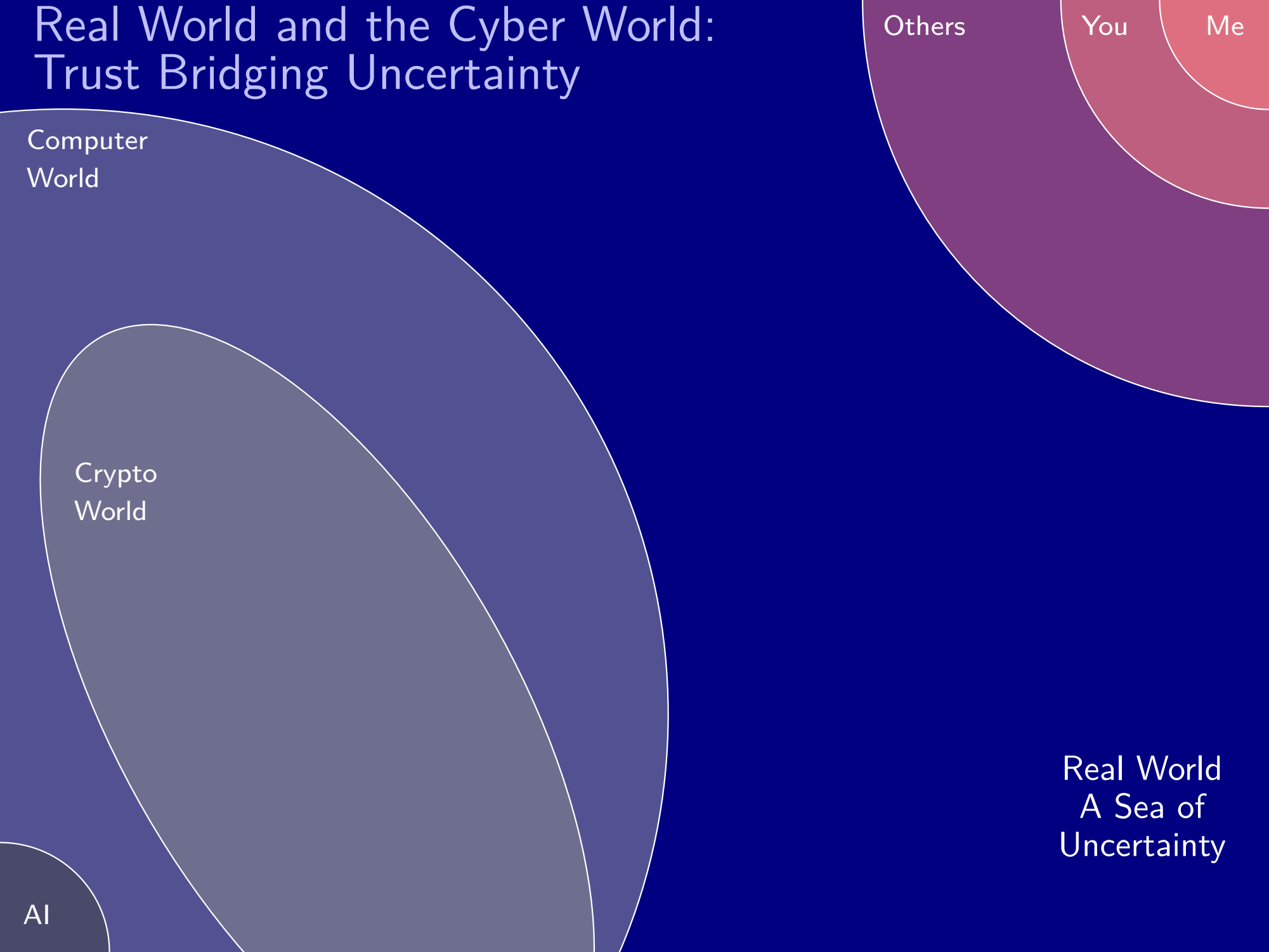
Real World and the Cyber World: Trust Bridging Uncertainty



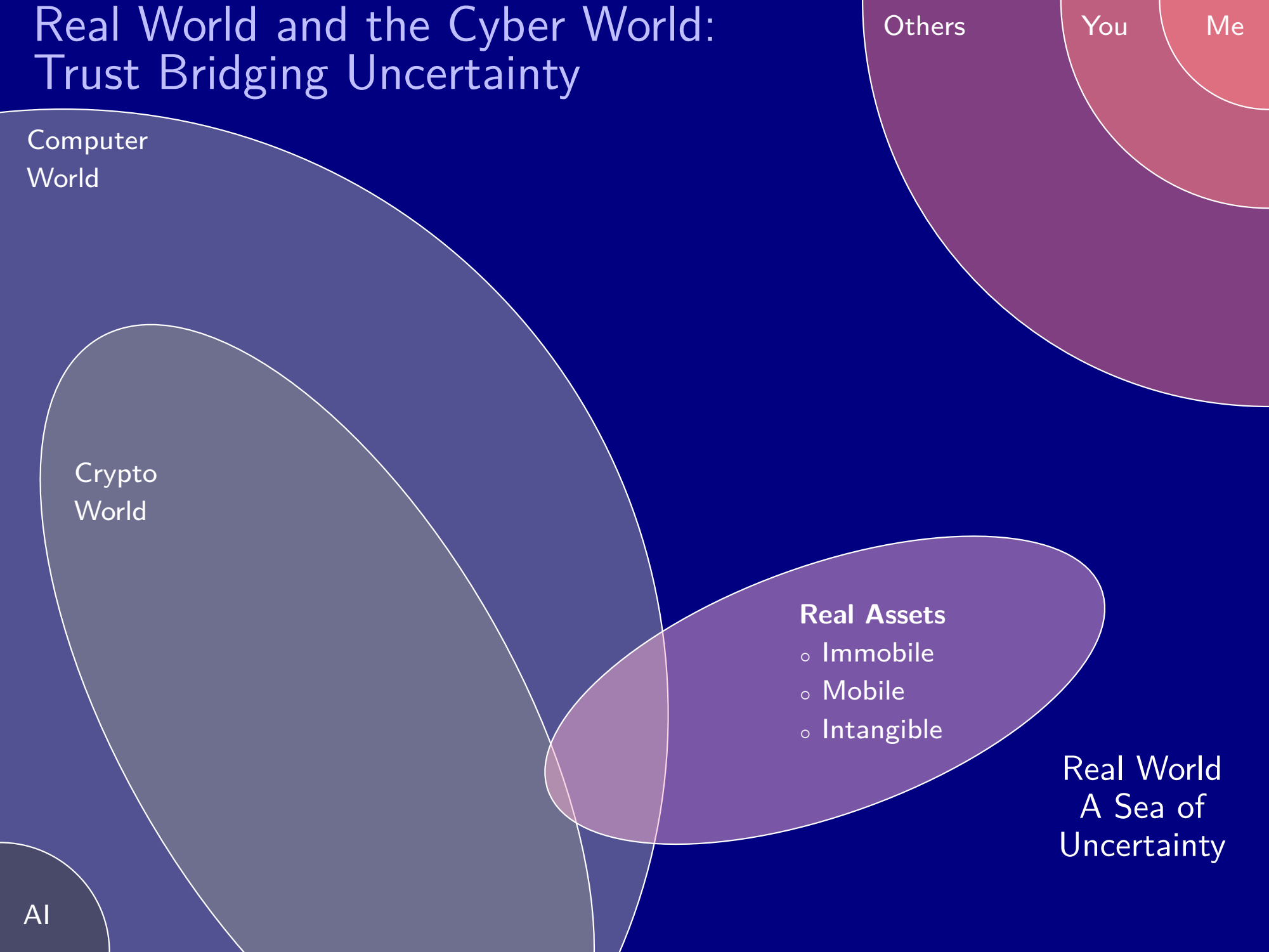
Real World and the Cyber World: Trust Bridging Uncertainty



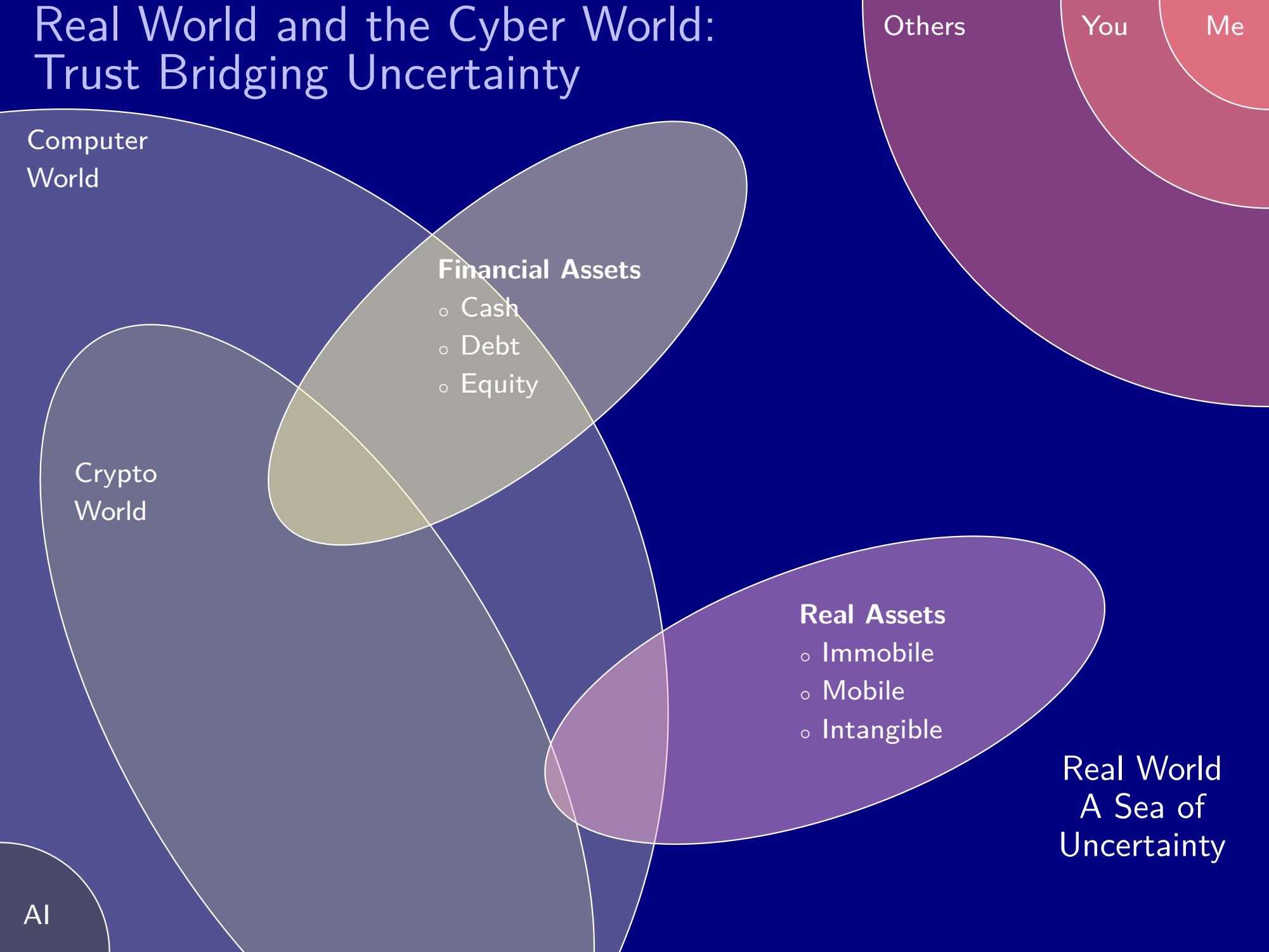
Real World and the Cyber World: Trust Bridging Uncertainty



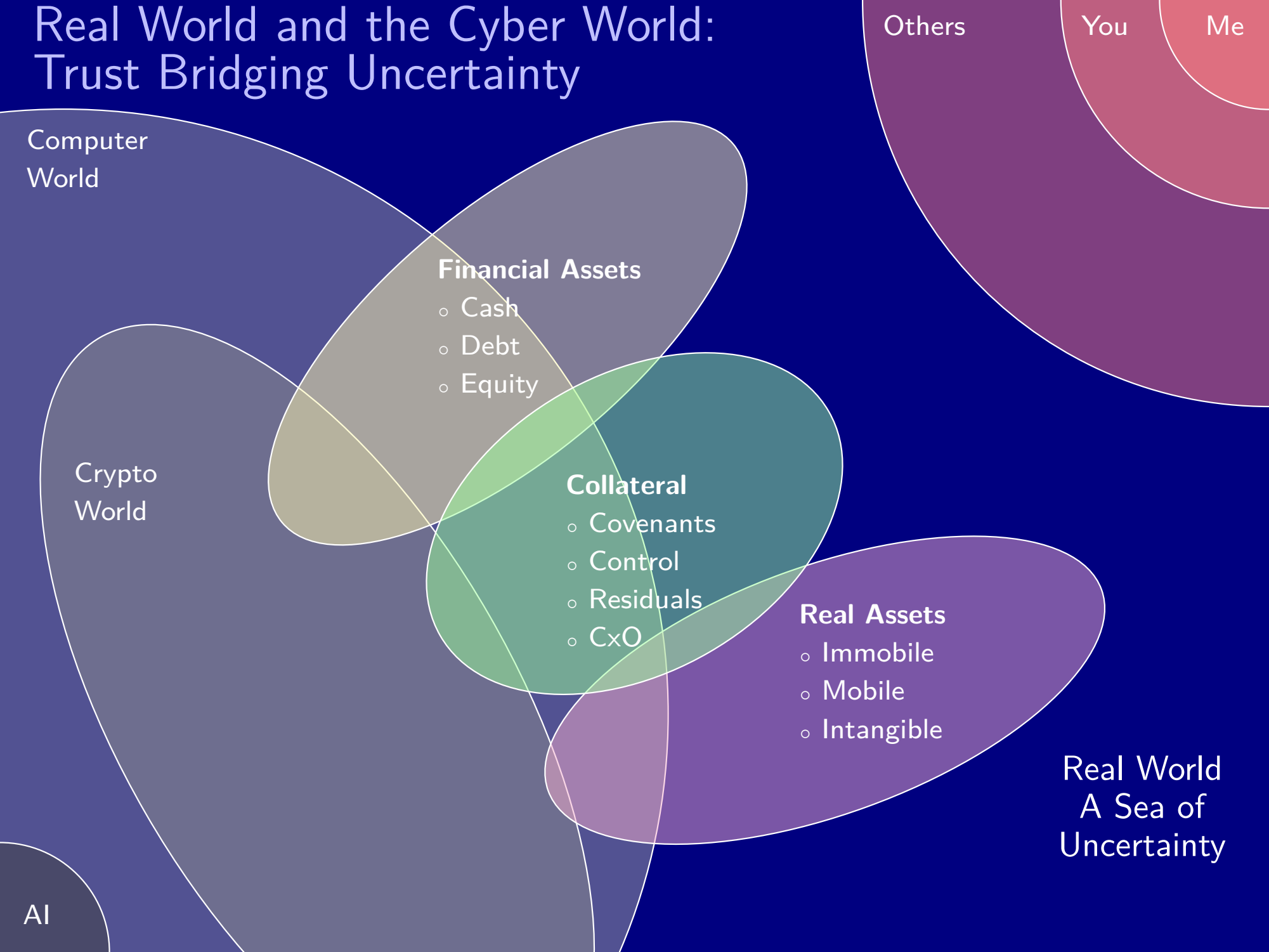
Real World and the Cyber World: Trust Bridging Uncertainty

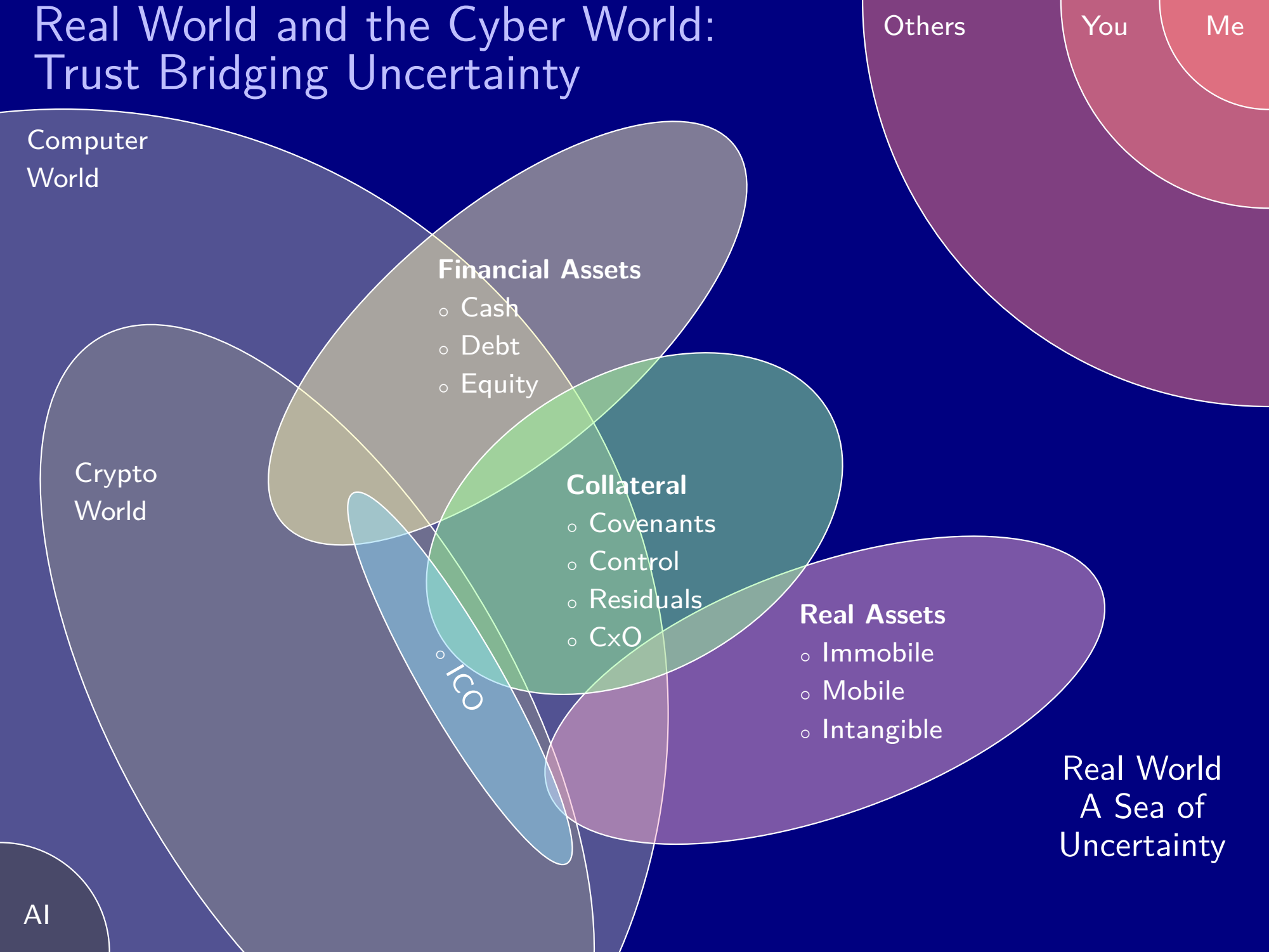


Real World and the Cyber World: Trust Bridging Uncertainty

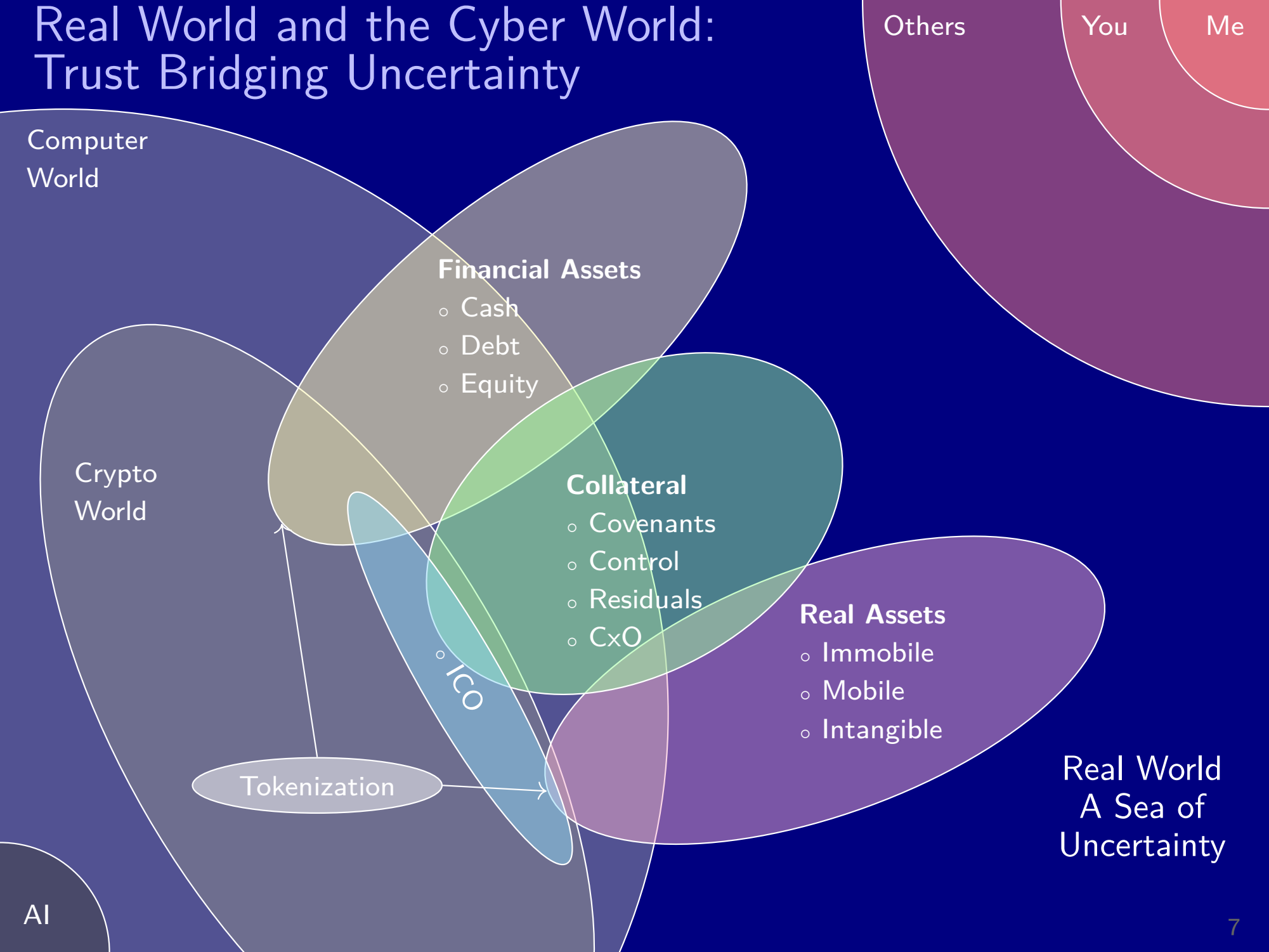


Real World and the Cyber World: Trust Bridging Uncertainty




Real World and the Cyber World:
Trust Bridging Uncertainty
Others
You
Me
Computer
World
Financial Assets
Cash
Debt
Equity
Crypto
World
Collateral
Covenants
Control
Residuals
CxO
ICO
Real Assets
Immobile
Mobile
Intangible
Real World
A Sea of
Uncertainty
AI

Real World and the Cyber World: Trust Bridging Uncertainty



Self-Sovereign Identity

Identity is Pluralistic and Relational

Relationship

- Family, Friend
- Social Media
- Civic, Professional
- Healthcare
- Commercial
- Financial
- Employment
- Government

Identity is Pluralistic and Relational

Relationship	**Role**
• Family, Friend	• Relative
• Social Media	• User
• Civic, Professional	• Member
• Healthcare	• Patient
• Commercial	• Customer
• Financial	• Debtor, Investor
• Employment	• Employee, M'ger
• Government	• Voter, Taxpayer

Identity is Pluralistic and Relational

Relationship	Role	Identity
• Family, Friend	• Relative	• Name
• Social Media	• User	• Login, Pseudonym
• Civic, Professional	• Member	• Name
• Healthcare	• Patient	• ID (HIPPA, PHI)
• Commercial	• Customer	• Age, Loyalty Pgm.
• Financial	• Debtor, Investor	• KYC, SSN
• Employment	• Employee, M'ger	• Name, EE ID, SSN
• Government	• Voter, Taxpayer	• Name, SSN

Attributes

- Inherent
  - DOB, height, finger prints, face scan, retina scan
- Accumulated
  - Health records, preferences, transaction history
- Assigned
  - SSN, telephone number, email

Identity Problems and Solutions

Problem	**Solution**
Unstructured data	Machine readable, schema, standardized
Changes in data	API to connect, authenticate, update
Authenticity	Digitally signed attestations
Self-asserted identity	Self-created public/private key pairs
Honey-pot repositories	Store data on edge devices, smart phones
Jurisdictional politics	Store data on edge devices, smart phones
Monopolistic control	Store data on edge devices, smart phones

Self-Sovereign Identity and Decentralized Identifiers (DIDs)

- Permanent
- Resolvable
- Cryptographically Verifiable
- Decentralized

Self-Sovereign Identity and Decentralized Identifiers (DIDs)

- Permanent
- Resolvable
- Cryptographically Verifiable
- Decentralized

"*No identifier in history has had all four of these properties—because what fundamentally enables DIDs is* ***blockchain technology***"

Drummond Reed, Decentralized Identifiers (DIDs) The Fundamental Building Block of Self-Sovereign Identity https://goo.gl/Au4uBx

Three Components of SSI

- Claims
- Proofs
- Attestations

SSI Solution

- Like the "drawer of important documents"
- Personal identity wallet on "edge" device = smart phone
- No massive central honey-pot repositories of PII data
- Start with **self-generated** = self-sovereign (a, A) private/public key pair
- Initially A is your secret. . . you choose how to share and combine
- You use A and other documentation to get attestations from trusted authorities
- Math chains of guarantees without degrading security: trust-chain

Christopher Allen Ten Commandments of SSI

1. **Existence.** Users must have an independent existence.
2. **Control.** Users must control their identities.
3. **Access.** Users must have access to their own data.
4. **Transparency.** Systems and algorithms must be transparent.
5. **Persistence.** Identities must be long-lived.
6. **Portability.** Information and services about identity must be transportable.
7. **Interoperability.** Identities should be as widely usable as possible.
8. **Consent.** Users must agree to the use of their identity and data.
9. **Minimalization.** Disclosure of claims must be minimized.
10. **Protection.** The rights of users must be protected.

https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2017/blob/master/topics-and-advance-readings/self-sovereign-identity-primer.md

Blockchain Technology and Self-Sovereign Identity

- Identity is immutable
- Blockchain stores self-created **public addresses**
- Blockchain provides guaranteed (distributed) access to **identifiers**
- Private key (off-chain) gives users ultimate control
- Everybody can access the information needed to verify credentials
- Users explicitly control data and access
- Verifiers can revoke credentials
- Separation of data storage and data verification

Zero Knowledge Proofs

Zero Knowledge Proofs

- It is possible to verify information without revealing it: a **zero knowledge proof**
- Where's Waldo with a mat

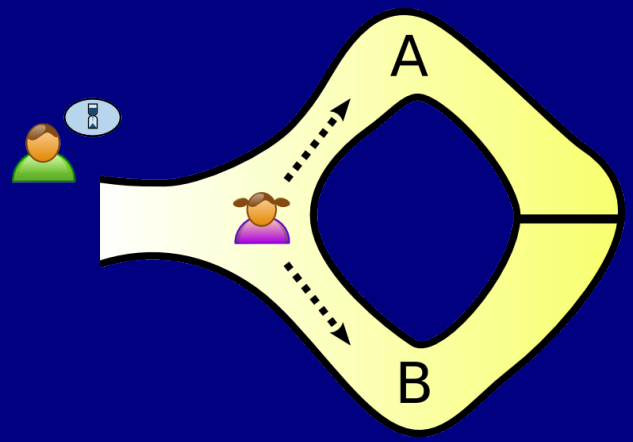


Figure 1: Alibaba's cave example: it is possible to prove you know something without revealing it.

Zero Knowledge Proofs

- Read-only access to private information, act and forget, rather than act and store
- Distributed database of all private credit, health, behavioral data
  - Owner grants **one-time**, **verify only** access to legitimate users
  - Underwrite an account from distributed data given permission; no questions!
  - User cannot pass along what they've learned
- Theoretic potential is huge
- Commercial development unclear: someone must profit for good idea to flourish