La confianza es la base de las sociedades modernas. Sin embargo, las relaciones basadas en confianza son difíciles de establecer y pueden ser explotadas fácilmente con resultados devastadores. En esta tesis exploramos el uso de protocolos criptográficos distribuidos para construir sistemas confiables donde la confianza se vea reemplazada por garantías matemáticas y criptográficas. En estos nuevos sistemas dinámicos, incluso si una de las partes se comporta de manera deshonesta, la integridad y resiliencia del sistema están garantizadas, ya que existen mecanismos para superar este tipo de situaciones. Por lo tanto, hay una transición de sistemas basados en la confianza, a esquemas donde esta mima confianza es descentralizada entre un conjunto de individuos o entidades. Cada miembro de este conjunto puede ser auditado, y la verificación universal asegura que todos los usuarios puedan calcular el estado final en cada uno de estos métodos, sin comprometer la privacidad individual de los usuarios.

La mayoría de los problemas de colaboración a los que nos enfrentamos como sociedad, pueden reducirse a dos grandes dilemas: el votar una propuesta, o un representante político, ó identificarnos a nosotros mismos como miembros de un colectivo con derecho de acceso a un recurso o servicio. Por ello, esta tesis doctoral se centra en los protocolos criptográficos distribuidos aplicados al voto electrónico y la identificación anónima.

Hemos desarrollado tres protocolos para el voto electrónico que complementan y mejoran a los métodos más tradicionales, y además protegen la privacidad de los votantes al mismo tiempo que aseguran la integridad del proceso de voto. En estos sistemas, hemos empleado diferentes mecanismos criptográficos que proveen, bajo diferentes asunciones, de las propiedades de seguridad que todo sistema de voto debe tener. Algunos de estos sistemas son seguros incluso en escenarios pos-cuánticos. También hemos calculado minuciosamente la complejidad temporal de los métodos para demostrar que son eficientes y factibles de ser implementados. Además, hemos implementados algunos de estos sistemas, o partes de ellos, y llevado a cabo una detallada experimentación para demostrar la potencial de nuestras contribuciones.

Finalmente, estudiamos en detalle el problema de la identificación y proponemos tres métodos no interactivos y distribuidos que permiten el registro y acceso anónimo. Estos protocolos son especialmente ligeros y agnósticos en su implementación, lo que permite que puedan ser integrados con múltiples propósitos. Hemos formalizado y demostrado la seguridad de nuestros protocolos de identificación, y hemos realizado una implementación completa de ellos para, una vez más, demostrar la factibilidad y eficiencia de las soluciones propuestas. Bajo este marco teórico de identificación, somos capaces de asegurar el recurso custodiado, sin que ello suponga una violación para el anonimato de los usuarios.